Tampereen yliopisto

Lasse Laukkanen

UHF RFID

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintyö
Heinäkuu 2019

TIIVISTELMÄ

Lasse Laukkanen: UHF RFID
Kandidaatintyö
Tampereen yliopisto
Tieto- ja sähkötekniikka, TkK
Toukokuu 2019

RFID on radiotaajuuksilla toimiva langaton etätunnistusmenetelmä. RFID-tunnistamisen tärkeimpänä ominaisuutena on, että radioaaltoja käytettäessä kohteiden tunnistaminen yksilöivästi ei vaadi suoraa näköyhtettä kohteen ja lukijan välillä. UHF RFID -järjestelmässä käytetään ultrakorkeiksi taajuuksiksi luokiteltua taajuusaluetta, eli UHF-taajuuksia. UHF-taajuudet mahdollistavat pienemmät antennit ja pitemmät lukuetäisyydet matalampiin taajuuksiin verrattuna.

RFID-järjestelmä koostuu yksinkertaisimmillaan lukijoista ja esineisiin kiinnitettävistä tunnisteista. RFID-tunnistamista voidaan käyttää esimerkiksi esineiden seuraamisessa tuotantolinjoilla, varastoissa ja autojen tiemaksujärjestelmissä. Hyödykkeiden seuraaminen RFID-järjestelmällä mahdollistaa automatisoidun tiedonkeräyksen esimerkiksi hyödykkeiden sijainnista, määrästä ja liikkumisesta tuotantolinjalla. Automaattinen tiedonkeruu vähentää manuaalista hyödykkeiden seurantaan kuluvaa työtä. Kerättyä tietoa voidaan käyttää parantamaan tuotannon tehokkuutta antamalla kontrollidataa tuotannonsuunnittelua varten. Automaattinen etätunnistaminen helpottaa ja tehostaa inventaarion hallintaa. Esimerkiksi varastotilassa olevien konttien sisältö ja määrä voidaan nopeasti saada selville RFID-tunnisteilla, koska tunnisteeseen voidaan tallentaa muokattavissa olevaa informaatiota siihen kiinnitetystä esineestä. Lisäksi tunnisteisiin on mahdollista kiinnittää sensorit, joilla voidaan esimerkiksi seurata realiajassa kiinitetyn kohteen lämpötilaa tai muuta tietoa.

UHF RFID -tunnisteet jaotellaan niiden virtalähteen mukaan kolmeen luokkaan, aktiivi, passiivi ja semiaktiivitunnisteisiin. UHF-taajuudet mahdollistavat halvat passiivitunnisteet, sekä usean tunnisteen samanaikaisen lukemisen. RFID-tunnisteissa on tyypilisesti mikrosiru ja muisti, joten ne kykenevät yksinkertaisiin laskuoperaatioihin ja tiedonsiirtoon molempiin suuntaan lukijan kanssa. RFID-järjestelmässä kontrollilaitteet, tyypillisesti tietokoneet, käyttävät radioaaltoja kommunikoimaan ympäröivän tilan esineiden kanssa, joissa on yhteensopiva RFID-tunnistelaite. Esineiden internetiin liittyy ajatus yksilöidysti tunnistettavissa olevista kohteista. RFID-tunnistaminen ja kommunikointi on mahdollinen teknologia esineiden internetin vaatimaan tunnistustarpeeseen.

Tämä kandidaatintyö käsittelee UHF RFID -teknologian perusperiaatteita. Perusperiaatteisiin katsotaan sisältyvän teknologioiden perusteet, jotka tarvitaan sähkömagneettisen säteilyn muokkaamiseen RFID-laitteelle tulkittavaksi signaaliksi. Työssä käsitellään lyhyesti RFID-laitteen toiminnan kannalta oleelliset asiat langattomasta tietoliikenteestä, kuten signaalin modulaatio ja RFID-tunnisteiden antennien perusperiaatteet. Lisäksi työssä käydään läpi tyypillisen UHF RFID -järjestelmän komponentit, RFID:n haasteita ja sovelluskohteita.

ALKUSANAT

Kandidaatintyön aihe valittiin ennaltamääritellystä aihepankista. Ajatusmallini oli, että kandidaatintyön aihevalinta toimi kannustimena tutkia itselleni vielä tuntematonta, mutta kiinnostavaa RFID-teknologiaa, sekä sivutuotteena saisin tuotettua kandidaatintyön opintoja varten. Tekstin kirjoittaminen oli mielekästä, mutta aiheen laajuuden vuoksi koin hankalaksi esittää aihemaailman perusperiaatteet ilman työn paisumista jättiläismäiseksi kandidaatintyön pituuteen suhteuttaen.

Haluan osoittaa suuret kiitokset tämän kandidaatintyön ohjaajalle Erja Sipilälle ohjauksesta, palautteesta ja neuvoista. Lisäksi kiitos kaikille mahtaville läheisilleni ja kavereilleni, jotka eivät menettäneet hermojaan altistuessaan suurelle määrälle yksinkertaisia tekstieditoriin liittyviä ”miten tämä tehdään” -kysymyksiä. Erityiset kiitokset ihanalle Marialle ja Lunalle tuesta, kannustuksesta ja läsnäolosta.

Tampereella, 30.6.2019

Lasse Laukkanen

SISÄLLYSLUETTELO

1. JOHDANTO 1
2. SÄHKÖMAGNEETTINEN SÄTEILY 2
2.1 Taajuus 2
2.2 Polarisaatio 4
3. ANTENNIT 5
3.4 Dipoliantenni 5
3.1 Antennin sähkökentät 7
3.2 Polarisaation vaikutus antennissa 7
3.3 Takaisinsironta 9
4. LANGATON TIEDONSIIRTO 12
4.2 Modulaatio 12
4.1 Signaalin tehospektri 14
4.3 Taajuuskaista 15
4.4 Määräykset 16
5. UHF RFID-TEKNOLOGIA 18
5.1 UHF RFID-järjestelmä 18
5.2 UHF RFID-tunniste 19
5.2.1 Passiivitunniste 20
5.2.3 Semipassiivitunniste 22
5.2.2 Aktiivitunniste 23
5.2.4 UHF RFID-tunnisteiden hinta 25
5.3 UHF RFID-lukijat 25
5.3.1 Lukulaitetyypit 25
5.3.2 RFID lukijan rakenne 27
5.4 Standardit 28
6. KÄYTTÖKOHTEET JA SOVELLUKSET 30
7. HAASTEET JA ONGELMAT 32
8. YHTEENVETO 35
LÄHTEET 36

LYHENTEET JA MERKINNÄT

ADC	engl. Analog Digital Converter, analogia-digitaalimuunnin
ASK	engl. Amplitude Shift Keying, amplitudisiirtoavainnus
BPSK	engl. Binary Phase Shift Keying, binäärivaihesiirtoavainnus
DAC	engl. Digital Analog Converter, digitaali-analogiamuunnin
DC	engl. Direct Current, tasavirta
FSK	engl. Frequncy Shift Keying, taajuussiirtoavainnus
HF	engl. High Frequency, korkea taajuus
I2C	engl. Inter-Integrated Circuit, kaksisuuntainen ohjaus- ja tiedonsiirtoväylä
IC	engl. Integrated Circuit, mikrosiru
IoT	engl. Internet of Things, esineiden internetti
ISO	engl. International Organization for Standards, kansainvälinen standardisointijärjestö
PSK	engl. Phase Shift Keying, vaihesiirtoavainnus
QAM	engl. Quadrature Amplitude Modulation, kvadratuuri amplitudimodulaatio
QPSK	engl. Quadrature Phase Shift Keying, kvadratuuri vaihesiirtoavainnus
RAM	engl. Random Access Memory, keskusmuisti
RFID	engl. Radio Frequency Identification, radiotaajuinen etätunnistus
ROM	engl. Read Only Memory, lukumuisti
UART	engl. Universal Asynchronous Receiver Transmitter, universaali asynkroninen lähetin-vastaanotin
UHF	engl. Ultrahigh Frequency, ultrakorkea taajuus

1. JOHDANTO

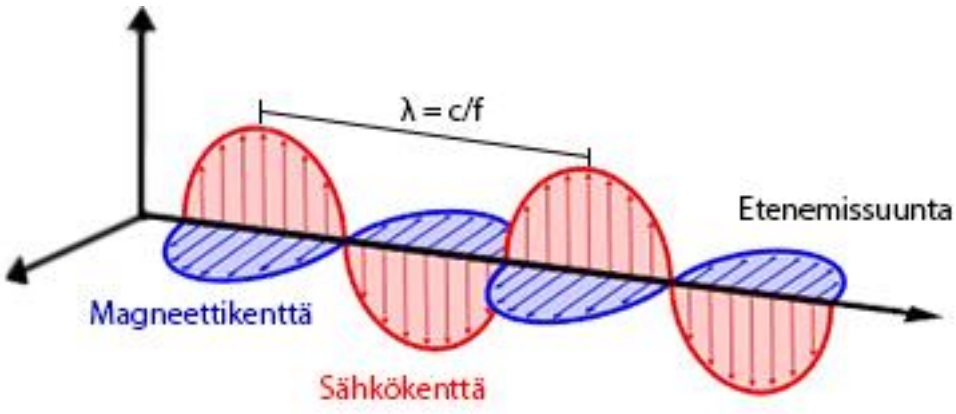
Kohteen yksilöivälle tunnistukselle on tarvetta monella toimialalla ja sovelluskohteissa. Suurivolyymisessa tuotantoympäristössä, jossa on tarvetta tunnistaa yksilöivästi jokainen tuote, on tehokkuuden vuoksi kriittistä automatisoida tunnistustoimenpide. Automaation kehittämisen ja työnkulun tehostamisen lisäksi kohteen yksilöivästä etätunnistamisesta on selkeitä hyötyjä. Jo toisessa maailmansodassa lentokoneissa käytettiin radiotaajuuiseen etätunnistukseen perustuvaa laitetta, transponderia. Transponderin vastaanottaessa radiosignaalin se lähettää takaisin lentokoneen yksilöivän tunnuksen sisältävän signaalin [1, s. 7]. Transponderin avulla viholliskone kyettiin erottamaan ystävällisestä koneesta.

RFID (engl. Radio Frequency Identification) eli radiotaajuinen tunnistus on langattomaan tietoliikenteesen perustuvaa teknologiaa, jonka avulla pystytään etänä tunnistamaan kohteita, kuten tavaroita tai jopa ihmisiä. RFID-järjestelmän ominaisuuksiin ja komponenttien rakenteeseen vaikuttaa suuresti sen käyttämä taajuusalue. Korkeiden taajuuksien käyttö mahdollistaa mataliin taajuuksiin verrattuna suuremmat tiedonsiirtonopeudet, pitemmät lukuetäisyydet, sekä helpommin ja halvemmin valmistettavat tunnisteet, eli tagit. UHF RFID -järjestelmät toimivat ultrakorkeiden taajuuksien alueella.

Tämän työn tavoite on kartoittaa UHF RFID -teknologiaan liittyvät perusperiaatteet ja samalla esitellä näkökulmia, joita järjestelmän kannalta on otettava huomioon. Toisessa luvussa käsitellään signaalien ymmärtämisen kannalta oleelliset asiat sähkömagneettisesta säteilystä. Kolmannessa luvussa tutustutaan UHF RFID -tunnisteiden antenneihin liittyviin käsitteisiin ja tyypilliseen passiivitunnisteissa käytettyyn antennityyppiin, dipoliantenniin. Neljännessä luvussa käsitellään langatonta tiedonsiirtoa taajuuden näkökulmasta. Viidennessä luvussa perehdytään UHF RFID -järjestelmän komponentteihin ja niiden toimintaperiaatteisiin, jotka nojautuvat aikaisemmissa luvuissa esitettyihin aiheisiin. Kuudennessa luvussa tutustutaan olemassa oleviin järjestelmiin ja sovelluskohteisiin. Seitsemännessä luvussa pohditaan mahdollisia UHF RFID -teknologian ongelmia ja haasteita. Kahdeksannessa luvussa on koottu yhteen tärkeimmät UHF RFID -teknologiaan liittyvät periaatteet.

2. SÄHKÖMAGNEETTINEN SÄTEILY

Radiosignaalit, eli radioaallot, ovat sähkömagneettista säteilyä. Sähkömagneettinen säteily koostuu kohtisuorassa etenemissuuntaansa nähden värähtelevistä sähkö- ja magneettikentistä ja se etenee valonnopeudella kuljettaen mukanaan säteilyenergiaa [2]. Sähkömagneettisella säteilyllä on aaltomaisia ominaisuuksia, joten sitä kutsutaan myös sähkömagneettiseksi aalloksi. Kuvassa 1 on esitetty sähkömagneettinen aalto, jonka etenemissuunta on kohtisuorassa sähkö- ja magneettikenttää vastaan. Yhden aallon pituutta on merkitty symbolilla *λ*.



Kuva 1. *Sähkömagneettinen aalto, perustuu [3, s. 36].*

Sähkömagneettinen aalto on jaksollinen signaali, joten sille on määriteltävissä aallonpituus ja taajuus. Seuraavissa luvuissa tarkastellaan RFID-järjestelmän kannalta kahta oleellista sähkömagneettisen aallon ominaisuutta, taajuutta ja polarisaatiota.

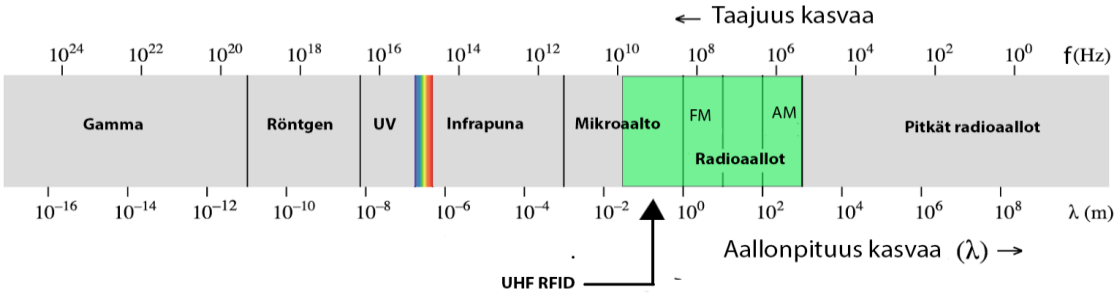
2.1 Taajuus

Sähkömagneettisen aallon taajuudella tarkoitetaan sitä, kuinka monta kertaa aalto värähtelee sekunnissa, eli värähtelynopeutta ja sitä merkitään usein symbolilla *f*. Sähkömagneettisen säteilyn taajuus määräytyy sen aallonpituudesta yhtälön 1

$$f = \frac{c}{\lambda} \tag{1}$$

mukaisesti, missä *f* on aallon taajuus, *c* aallon etenemisnopeus, eli valonnopeus tyhjiössä ja *λ* aallonpituus [4, s. 1077]. Sähkömagneettisten aaltojen jako taajuuden tai aallonpituuden mukaan voidaan esittää spektrinä, jossa eri taajuusalueet ovat nimettyjä [5, s. 10]. Sähkömangeettisen säteilyn spektri on esitettynä kuvassa 2, jossa korostettuna ovat spektrin alueet, joilla UHF RFID-järjestelmät toimivat.

Eri standardit ja tahot saattavat nimittää eri taajuusaleuita toisistaan poiketen. UHF-taajuusalueella radioaaltoja korkeampia taajuuksia nimitetään myös mikroaalloiksi [5, s. 11].



Kuva 2. *Sähkömagneettisen säteilyn spektri, perustuu [5, s. 10].*

Taulukossa 1 on esitettynä sähkömagneettisen säteilyn spektrin radioaaltojen taajuusalue. Taulukossa ultrakorkeiksi taajuuksiksi (UHF, engl. Ultra High Frequency) on luokiteltu taajuudet 300 MHz – 3 GHz [5, s. 10]. Riippuen standardista, radioaaltojen nimet ja rajat saattavat poiketa.

Taulukko 1. *Radioaaltojen taajuusalueen nimitykset [6, s. 11].*

Lyhenne	Taajuusalueen nimi	Taajuusalue	Aallonpituus
VLF	Very Low Frequency	3 kHz – 30 kHz	100 km – 10 km
LF	Low Frequency	30 – 300 Hz	10 km – 1 km
MF	Medium Frequency	300 kHz – 3 MHz	1 km – 100 m
HF	High Frequency	3 MHz – 30 MHz	100 m – 10 m
VHF	Very High Frequency	30 MHz – 300 MHz	10 m – 1 m
UHF	Ultra High Frequency	300 MHz – 3 GHz	1 m – 10 cm
SHF	Super High Frequency	3 Ghz – 30 Ghz	10 cm – 1 cm
EHF	Extremely High Frequency	30 GHz – 300 GHz	1 cm – 0,1 cm

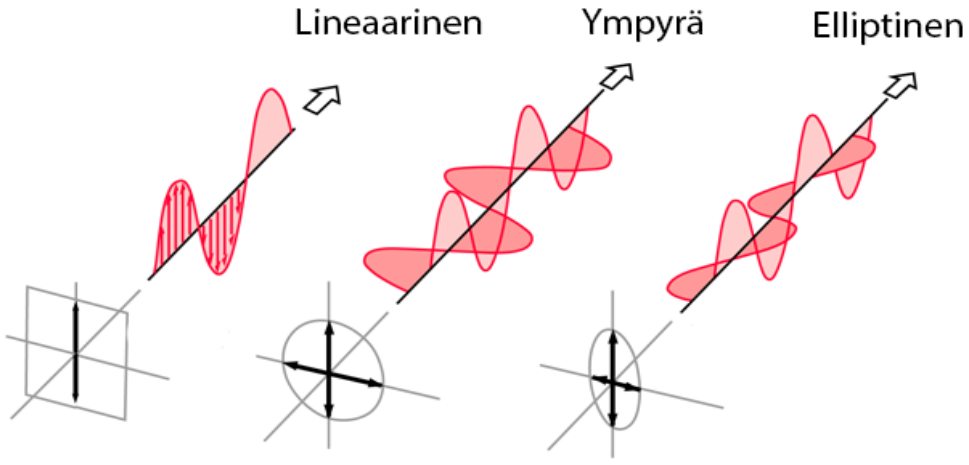
Valtaosa kaupallisista UHF RFID-järjestelmistä käyttää radiokanavana radiotaajuuksia väliltä 860 – 960 MHz [7, s. 12]. RFID-järjestelmän taajuusalue vaikuttaa merkittävästi radiolaitteen ominaisuuksiin ja vaatimuksiin. Signaalin taajuus vaikuttaa RFID-järjestelmän lukuetäisyyteen, tiedonsiirtonopeuteen, radioaaltojen etenemiseen ja antennien kokoon. Tietyillä taajuusalueilla operointi voi valtiokohtaisesti olla

luvanvaraista, joten laitteiston taajuusalue täytyy ottaa huomioon RFID-järjestelmää hankittaessa.

2.2 Polarisaatio

Sähkömagneettisen aallon polarisaatio kuvastaa, kuinka sähkökenttävektorin suunta ja amplitudi käyttäytyvät ajassa sen etenemissuuntaan kohtisuorassa olevaan tasoon nähden. Polarisaatio siis ilmaisee amplitudin suuntariippuvuutta etenemissuuntaansa nähden. Polarisaation erikoistapauksia ovat lineaarinen, ympyrä- ja elliptinen polarisaatio. [8, s. 71]

Sähkökentän värähdellessä vain yhteen suuntaan amplitudin pysyessä vakiona sähkömagneettisen aallon kutsutaan olevan lineaarisesti polarisoitunut. Ympyräpolarisaatiossa sähkökenttä kiertyy tasaisella kulmanopeudella ympäri etenemissuuntaansa nähden kohtisuoraan olevassa tasossa. Elliptisesti polarisoituneessa aallossa aallon amplitudi on ajasta ja paikasta riippuvainen ja kiertyy ympyräpolarisaation tavoin. [8, s. 68] Kuvassa 3 ovat esitettyinä polarisaation erityistapaukset ja poikkileikkauskuvio sähkömagneettiselle aallolle, missä vasemmalla on lineaarinen polarisaatio, keskellä ympyräpolarisaatio ja oikealla elliptinen polarisaatio.



Kuva 3. *Sähkömagneettisen aallon polarisaation erityistapaukset, perustuu [9].*

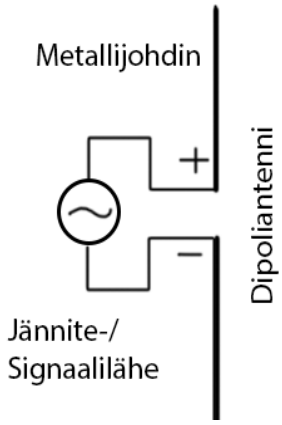
Polarisaatiolla on suuri merkitys RFID-sovelluksissa antennien valinnan kannalta. Polarisaatio vaikuttaa esimerkiksi tunnisteen antennin kykyyn vastaanottaa signaali, joten antennin polarisaatio on otettava huomioon järjestelmän suunnittelussa.

3. ANTENNIT

Antenni on laite, joka muuntaa siihen johdetut sähköiset signaalit sähkömagneettisiksi aalloiksi, sekä vastaanottaa sähkömagneettisia aaltoja muuntaen ne takaisin sähköisiksi signaaleiksi. Yksinkertaisena antennina toimii esimerkiksi tavallinen metallijohdin. Ajassa muuttuva sähköinen signaali, esimerkiksi sinimuotoinen sähkövirta, luo johtimen ulkopuolelle sähkömagneettisia aaltoja, jotka indusoivat, eli synnyttävät jännitteen vastaanottavassa antennissa [10, s. 108]. Indusoitunut jännite puolestaan synnyttää vaihtosähkövirran antennin virtapiiriin. Indusoitunut jännite saa aikaan vastaanottajan päässä sähkövirran. Vastaanotettu jännite on taajuudeltaan sama kuin lähetetty ja sen suuruus on kääntäen verranollinen antennien väliseen etäisyyteen [1, s. 52].

3.4 Dipoliantenni

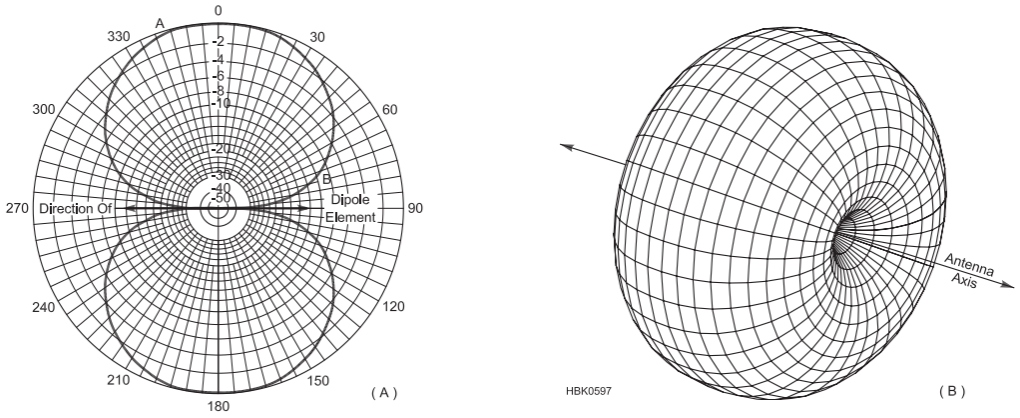
Dipoliantennin rakenne on yksinkertainen ja se koostuu yksinkertaisimmillaan kahdesta vastakkaisiin suuntiin erkanevasta johtimesta. Puoliaaltodipoliantenni on yleisin RFID-tunnisteissa käytetty antenni ja sen pituus on lähes puolet radioaallon pituudesta [8, p. 182]. Puoliaaltodipoliantennin pituus 900 MHz taajuudella on noin 15 cm ja 2,4 GHz taajuudella noin 6 cm [1, s. 29]. Kuvassa 4 on esitetty puoliaaltodipolin periaatekuva. Antenni koostuu kahdesta metallilangasta, joihin on kytketty jännitelähde. Jännitelähteen tarkoitus on synnyttää jännitesignaali, jonka antenni lähettää ympäröivään tilaan.



Kuva 4. *Puoliaaltodipoli, perustuu [1, s. 27].*

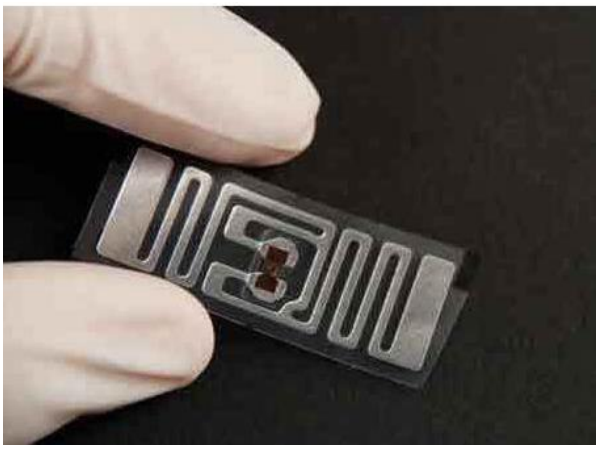
Antennin säteilykuvio ilmaisee antennin säteilemän tehon ympäröivään tilaan [1,s. 77]. Rakenteeltaan erilaisilla antenneilla on erilainen säteilykuvio, joten antennityypin valinnalla voidaan vaikuttaa antennin suuntaavuuteen. Säteilykuvion ulkopuolella signaali on vaimentunut vahvasti ja peittynyt muuhun kohinaan, jolloin signaalia ei voida

helposti tulkita [8, s. 80]. Kuvassa 5 vasemmalla on dipoliantennin säteilykuvion poikkileikkaus ja oikealla kolmiulotteinen aproksimaatio.



***Kuva 5**. Diboliantennan säteilykuvio [11] .*

Käytännössä UHF RFID -tunnisteissa käytetään erilaisia variaatioita dipoliantennista [1, s. 27]. RFID-tunnisteen suurin komponentti on sen antenni. Tunnisteen halutaan tyypillisesti olevan huomaamaton ja kasvava tarve mobiilijärjestelmissä yhä pienemmille antennirakenteille asettaa vaatimuksia dipoliantennin koolle, jolloin 15 cm pitkä suora dipoliantenni ei välttämättä ole soveltuva kaikkiin järjestelmiin. Kuvassa 6 on esitetty kaupallinen UHF RFID -tunnisteen antenni. Antennin koko on saatu lyhyemmäksi mutkittelemalla johdinta.

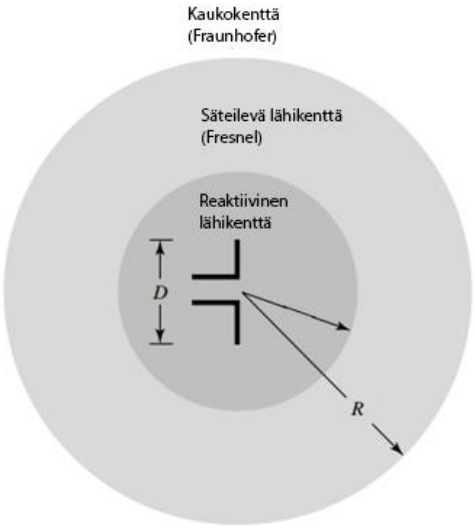


***Kuva 6**. Mutkitteleva puoliaaltodipoliantenni [11].*

Antennin lähettämän tai vastaanottaman signaalin aallonpituus, ja samalla signaalin taajuus, on riippuvainen antennin fyysisestä koosta. Tekemällä dipoliantenniin mutkia, sen pituus saadaan lyhyemmäksi muuttamatta suurelti antennin taajuusaluetta. Sähkövirta luo johtimen ympärille sähkömagneettisen kentän, jolloin mutkittelevassa rakenteessa on käytettävä erilaisia monimutkaisia tekniikoita kompensoimaan häiriötä aiheuttavia vastakkaissuuntaisia sähkökenttiä. [1, s. 309]

3.1 Antennin sähkökentät

Antennin ympärilleen luoma sähkömagneettinen kenttä jaetaan usein sähkömagneettisten ominaisuuksien perusteella kolmeen alueeseen [8, s. 34]. Kuvassa 7 on esitetty antennin sähkömagneettisen kentän alueet, joita ovat reaktiivinen lähikenttä, säteilevä lähikenttä eli Fresnellin alue ja kaukokenttä eli Fraunhoferin alue.



Kuva 7. *Antennin sähkömagneettiset kentät, perustuu [8, s. 34].*

Kaukokentän etäisyydellä aallon sähkö- ja magneettikentän jakautuminen on tasoittunut ja se etenee vapaan tilan tasoaaltona, eikä antenni vaikuta aallon etenemiseen. Kaukokentän alue voidaan tulkita alkavan etäisyydestä *R*, jossa säteilevä lähikenttä päättyy, yhtälön

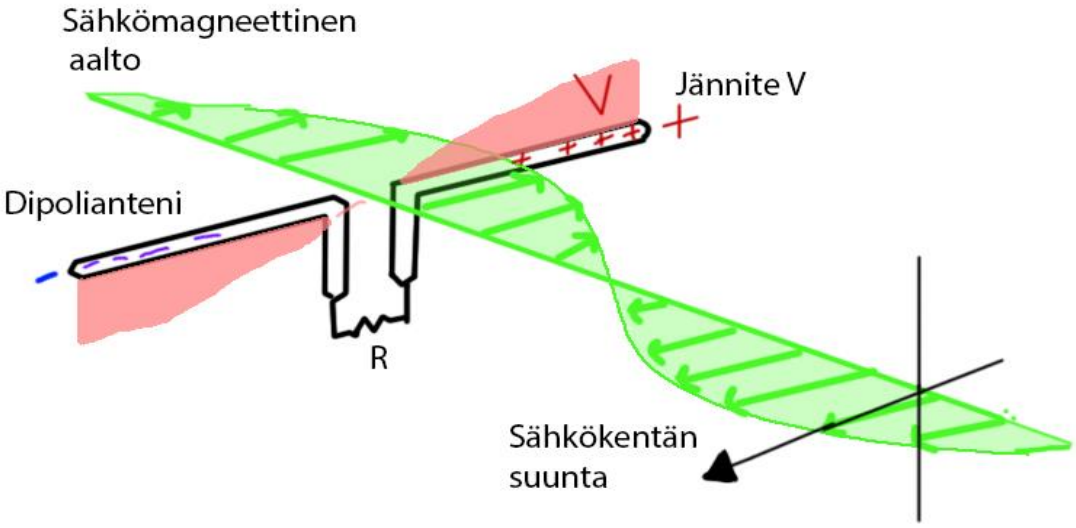
$$R = \frac{2 * D^2}{\lambda} \tag{2}$$

avulla, missä *D* on antennin pituus ja *λ* signaalin aallonpituus. [8, s. 34] Järjestelmän rakenne ja toiminta riipuu siitä, operoiko se kauko- vai lähikentässä. Korkeataajuiset järjestelmät, kuten UHF RFID -järjestelmä, yleisesti ottaen toimivat kaukokentässä, mahdollistaen pitemmän lukuetäisyyden ja suuremman siirtonopeuden kuin matalilla taajuuksilla ja lähikentässä toimivat järjestelmät. [10, s. 342]

3.2 Polarisaation vaikutus antennissa

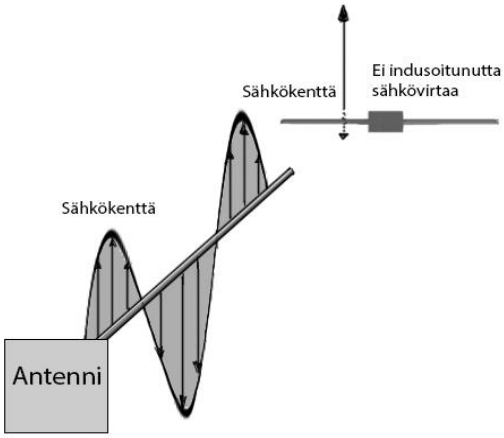
Kohdatessaan antennin muuttuva sähkökenttä saa aikaan vastanottavassa antennipiirissä sähkövirran liikuttamalla antennissa elektroneja edestakaisin [2, s. 24]. Kuvassa 8 on esitettynä dipoliantenni, jonka kohdannut muuttuva sähkökenttä työntää elektroneja edestakaisin antennissa vastuksen R läpi, joka voidaan tulkita esimerkiksi radiovastaanottimeksi. Liikkuvat elektronit ovat sähkövirtaa, joka tulkitaan signaaliksi.

Lineaarisesti polarisoitunut sähkökenttä on antennin suuntainen, jolloin koko kenttä vaikuttaa elektronien liikuttamiseen [1, s. 86].



Kuva 8. *Sähkömagneettinen aalto indusoi virran dipoliantenniin, perustuu [1, s. 86]*

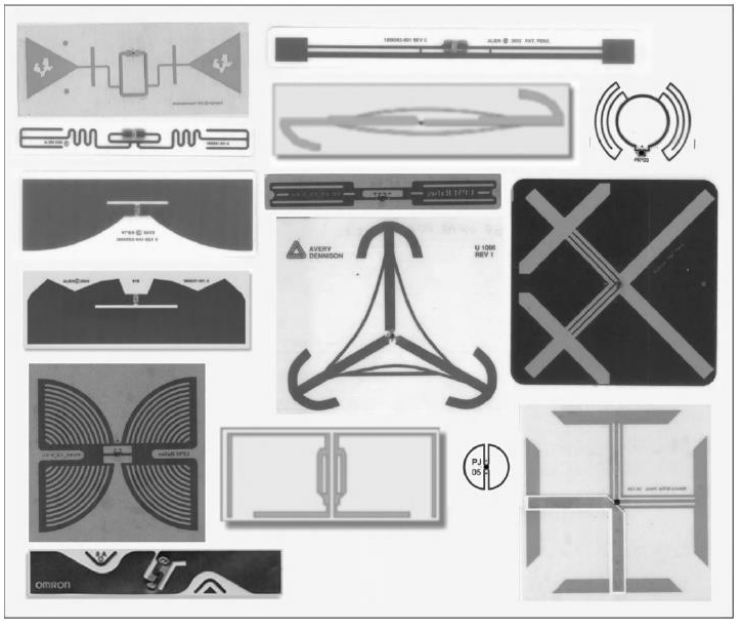
Polarisaatiosta johtuen antennit pystyvät vastaanottaman signaalin parhaiten, kun sen antennielementit on polarisoitu vastaanotettavan signaalin polarisaation mukaisesti [12, s. 827]. Kuvassa 9 on esitetty lähettävä antenni, jonka radioaalto on suunnattu vastaanottavaan antenniin siten, että vastaanotettava sähkökenttä on kohtisuorassa vastaanottajan antenniin. Kuvan antennissa ei indusoidu virtaa, eikä signaalia kyetä havaitsemaan.



Kuva 9. *Kohtisuorasti vastaanottavaan antenniin polarisoitunut sähkökenttä, perustuu [1, s. 87].*

Kuvan 9 tapauksessa antennin ja vastaanotettavan signaalin polarisaatio ovat kohtisuorassa siten, että vastaanottavassa antennissa sähkömagneettinen aalto ei saa

aikaan antennin elektronien liikkumista antennin pituussuunnassa, vaan poikittaisesti. Tällöin signaali ei synnytä antennin piirissä virtaa, eikä lukulaite kykene havaitsemaan saapuvaa signaalia [12, s. 827]. Kuvassa 10 on esitettynä kaupallisia UHF-tunnisteita, joissa on yksinkertaisen dipoliantennin lisäksi monimutkaisempia antenniratkaisuja. Monimutkaisella rakenteella on pyritty mm. ratkaisemaan polarisaation aiheuttamia ongelmia.



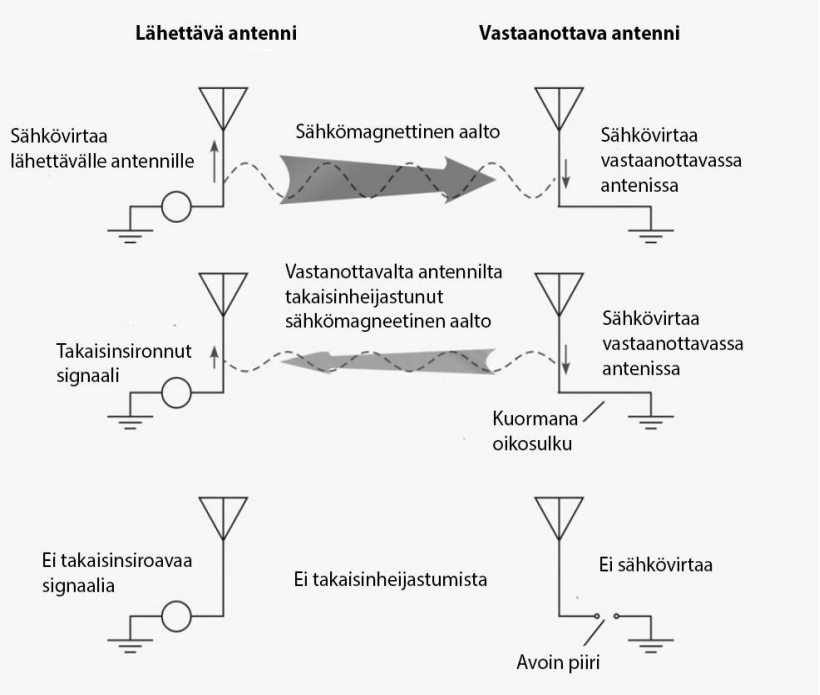
Kuva 10. *Kaupallisia UHF RFID-tunnisteita [1, s. 300].*

Polarisaation merkitys on otettava huomioon varsinkin UHF-tunnisteiden antenneissa, sillä jos antennin rakenne koostuu suorista metallijohtimista, signaalin vastaanottaminen saattaa olla mahdotonta polarisaation ollessa epäsuotuisa.

3.3 Takaisinsironta

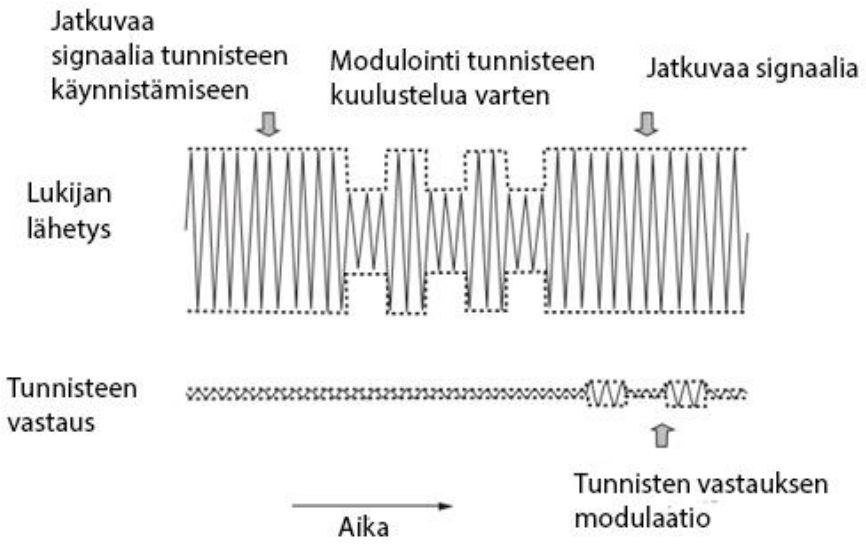
Passiivisessa UHF RFID -tunnisteessa ei ole erillistä virtalähdettä, joten se ei myöskään kykene luomaan itse radiosignaalia. Sen sijaan passiivitunniste hyödyntää tiedonsiirrossa lukijan lähettämää sähkömagneettista signaalia. UHF RFID -passiivitunnisteen ja -lukijan välisessä kommunikaatiossa lukijan lähettävän antennin sähkömagneettinen säteily indusoi jännitteen vastaanottavassa antennissa. Indusoitunut jännite synnyttää vastaanottavassa piirissä virran. Vastaanotetun signaalin synnyttämä sähkövirta lähettää nyt vastaanottajan antennissa ympärilleen sähkömagneettista säteilyä, jonka lukijan antenni puolestaan vastaanottaa indusoiden jännitteen takaisin lukijassa. [1, s. 65] Tätä sähköisen signaalin takaisinheijastumista kutsutaan takaisinsironnaksi (engl. Backscattering).

Kuvassa 11 on esitettynä yksinkertaistettu toimintaperiaate signaalin takaisinsironnasta. Lähetetty signaali palaa takaisin lähettäjälle hieman heikentyneenä, kun vastaanottavassa piirissä antenni on kytkettynä suoraan maahan. Kuvan alimmassa tilanteessa kuorma on katkaistu, jolloin lähettävään antenniin ei indusoidu takaisinsiroavasta signaalista jännitettä vastaanottavan laitteen antennipiirin virran ollessa nolla.



Kuva 11. *Takaisinsironnan periaate, perustuu [1, s. 65].*

Kuvassa 12 on esitettynä periaatteellinen tyypillinen yhteystapahtuma lukijan ja passiivisen RFID-tunnisteen välillä. Aluksi lukija lähettää jatkuva-aikaista signaalia, jonka lähialueen kaikki tunnisteet vastaanottavat ja saavat siitä tarvitsemansa tehon käynnistyäkseen. Sen jälkeen lukija lähettää moduloidun viestisignaalin, joka on kohdistettu vain halutulle tunnisteelle. Vastaanottava tunniste muuttaa antennin impedanssia lähetettävän viestin bittisekvenssin mukaisesti, jonka vastaanottava antenni tulkitsee tunnisteelta takaisinsiroavasta moduloidusta signaalista. [10, s. 341]



Kuva 12. *Lukutapahtuma: passiivitunnisteen käynnistys, tunnistus ja lukeminen, perustuu [5, s. 341].*

Takaisinsiroavaan signaalia hyödynnetään välittämään lähettävältä laitteelta saatua informaatiota vastaanottajalle. Informaatio saadaan sisällytettyä takaisinsiroavaan signaaliin moduloimalla lähetettävää signaalia. Modulaatiota käsitellään seuraavassa luvussa.

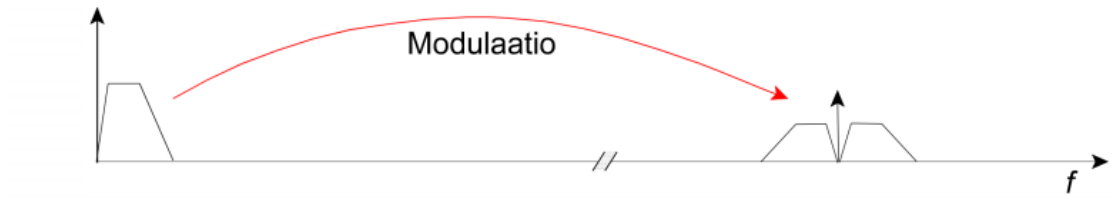
4. LANGATON TIEDONSIIRTO

Kuljettaakseen mukanaan tietoa radioaaltona liikkuvassa signaalissa on tapahduttava muutoksia. Tyypillisesti langattomissa järjestelmissä käytetään modulaatioksi kutsuttua tekniikkaa, jossa yhteen signaaliin lisätään toinen tietoa sisältävä signaali. Useimmiten modulaation tuloksena on signaalin taajuusalueen siirtyminen.

4.2 Modulaatio

Modulaatiolla tarkoitetaan prosessia, missä informaatio muokataan tietoliikennekanavaan lähetettäväksi sopivaan muotoon. Modulaatio voi olla analoginen tai digitaalinen. Analogisessa modulaatiossa jatkuva-aikainen kantataajuinen signaali voidaan siirtää korkeatajuiseen kantoaaltosignaaliin. Digitaalisessa modulaatiossa bittimuodossa oleva data saadaan kuvattua jatkuva-aikaiseksi aaltomuodoksi. [2, s. 165] Viestisignaalin kommunikaatiokanava saattaa aiheuttaa vaimentumista tietyillä taajuusalueilla. Järjestelmän käyttäessä vain tietyn taajuisia signaaleita järjestelmän tiedonsiirtonopeus on hyvin rajoittunut, koska tällöin kanava ei kykene kuljettamaan samanaikaisesti informaatiota eri suuntiin samantaajuisten signaalien sekoittuessa keskenään. Langattomassa kanavassa eri taajuusalueet ovat jaettu tiettyjen järjestelmien käyttöön, jolloin signaali on siirrettävä halutulle toiminta-alueelle.

Kantoaalto on vakiotaajuuksinen signaali, mihin viestisignaalin informaatiosisältö sisällytetään moduloimalla. Koska kantoaallon signaali voidaan valita, voidaan viestisignaalin taajuusalue siirtää taajuustasossa käyttämällä tietyn taajuista kantoaaltoa. [2, s.170] Kuvassa 13 on esitettynä matalalla taajuudella olevan viestisignaalin siirtäminen taajuustasossa korkeammalle modulaation seurauksena.

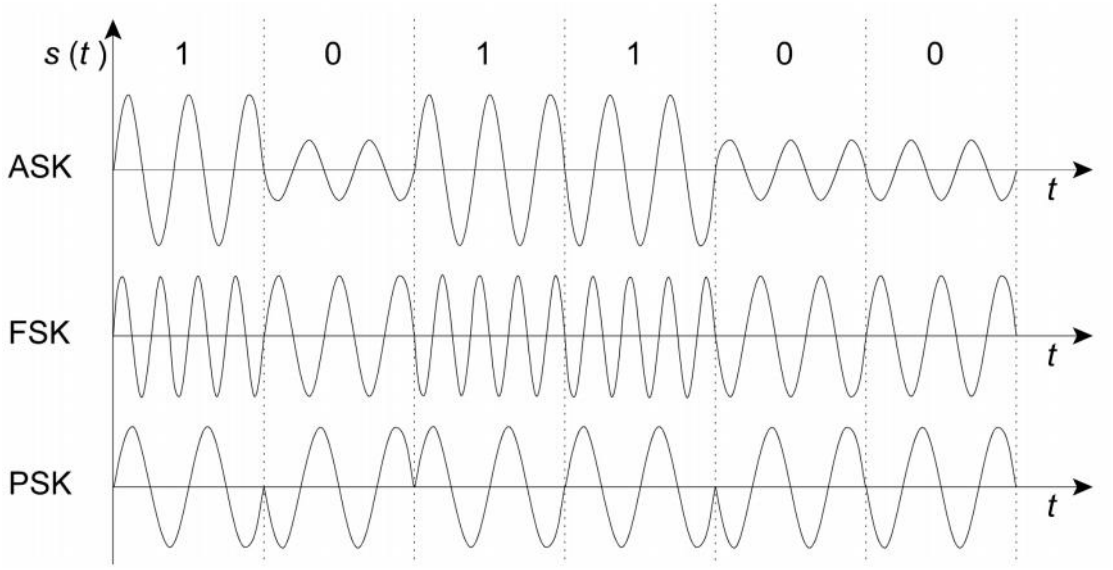


Kuva 13. *Viestisignaalin taajuussiirto.*

Kantoaallon käytöstä on suurta etua, koska lähetettävän moduloidun viestisignaalin taajuus voidaan asettaa halutuksi. Korkeataajuiset signaalit mahdollistavat mm. rakenteeltaan pienkokoisten antennien käyttämisen. Kantoaallon valitsemisella voidaan asettaa signaalin taajuus jonkin järjestelmän käyttämälle taajuusalueelle ja lisäksi

käytetty kanava voidaan jakaa taajuuskanaviin mahdollistaen usean signaalin samanaikaisen välittämisen. [13]

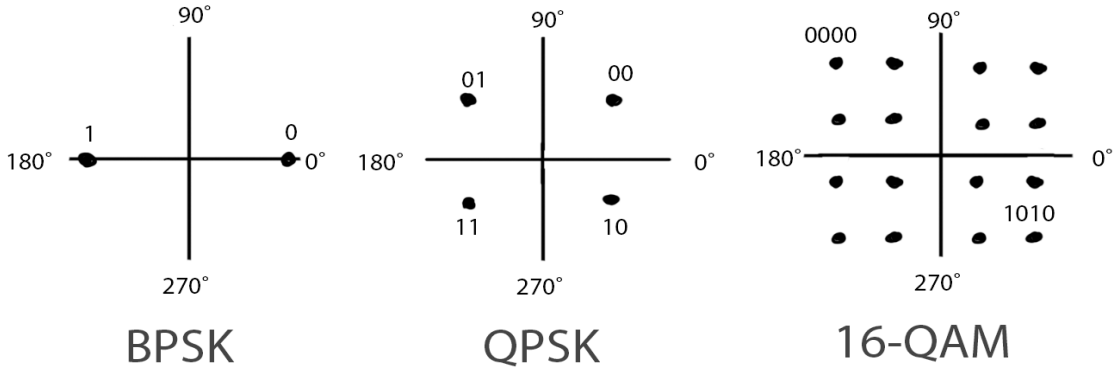
Digitaalisissa perusmodulaatiotekniikoissa kantoaallon jotakin ominaisuutta, kuten vaihetta, amplitudia tai taajuutta muokataan bittijonon mukaisesti. Kuvassa 14 on esitetty tyypillisiä digitaalisia modulaatiotekniikoita, joista RFID -järjestelmille oleellisia ovat amplitudisiirtoavainnus (ASK, engl Amplitude Shift Keying), taajuussiirtoavainnus (FSK, engl. Frequency Shift Keying) ja vaihesiirtoavainnus (PSK, engl. Phase Shift Keying). ASK:ssa kantoaallon amplitudi vaihtelee kahden arvon välillä riippuen bitin arvosta. FSK:ssa kantoaallon taajuus vaihtelee kahden eri arvon välillä. PSK:ssa kantoaallon vaihekulmaa vaihdellaan riippuen lähetettävästä bitistä. [14, s. 111].



Kuva 14. *Tyypillisiä digitaalisia modulaatiotekniikoita.*

Tiedonsiirtonopeutta voidaan parantaa lähettämällä yksittäisten bittien sijaan symboleja, jotka esittävät useaa bittiä kerrallaan. Amplitudin lisäksi saman kantoaallon vaihetta voidaan moduloida, jolloin symbolit voidaan tulkita vaiheen ja amplitudin hahmottavassa jännitteen osoittimia käyttävästä konstellaatiokartasta, kuten kuvassa 15 on esitetty. Kuvassa on myös esitetty kvadratuurivaihesiirtoavainnus (QPSK, engl. Quadrature Phase Shift Keying), binäärivaihesiirtoavainnus (BPSK, engl. Binary Phase Shift Keying) ja 16-kvadratuuriamplitudimodulaatio (16-QAM, engl. Quadrature Amplitude Modulation) modulaatiotekniikoiden konstellaatiokartat. BPSK:ssa loogiselle 1 ja 0:lle on molemmille yksi symboli, kun taas QPSK:ssa on käytössä 4 symbolia, joista jokainen kuvaa kaksi bittiä kerrallaan. 16-QAM modulaatiossa yhteen symboliin on käytetty neljä bittiä. Symbolien määrän kasvaessa kohinasta aiheutuvat mahdolliset häiriöt myös kasvavat, koska jokin signaali saattaa siirtyä kohinasta johtuen toisen symbolin alueelle. [12, s.

381] Kuvan modulaatiotekniikat ovat teknisesti ja laskennallisesti monimutkaisempia kuin ASK, FSK ja PSK, joten ne asettavat laitteistolle korkeammat vaatimukset.



Kuva 15. *Konstellaatiokuvat BPSK, QPSK ja 16-QAM modulaatioille.*

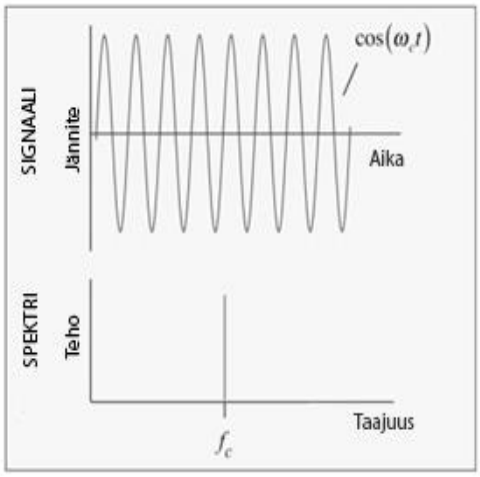
RFID-järjestelmän käsittelemät signaalit ovat tyypillisesti digitaalisesti moduloituja [1, p. 56]. Tiedonsiirtoa varten radioteitse on tarpeellista siirtää haluttu bittisekvenssi analogiseksi radiosignaaliksi. RFID -tunnisteen muistista halutaan lukea informaatiota, joka on talletettu digitaalisessa muodossa eli bitteinä. Tunnisteen muistista saadulla bittijonolla moduloimaan lukulaitteelle radioteitse lähtevä analoginen signaali [1, s. 199]. Tyypillisesti passiiviset UHF RFID -tunnisteet käyttävät ASK-modulaation variaatioita [15, s. 37].

4.1 Signaalin tehospektri

Signaali *V*, joka on jaksollinen ja aikariippuvainen, voidaan esittää yhtälöllä 3

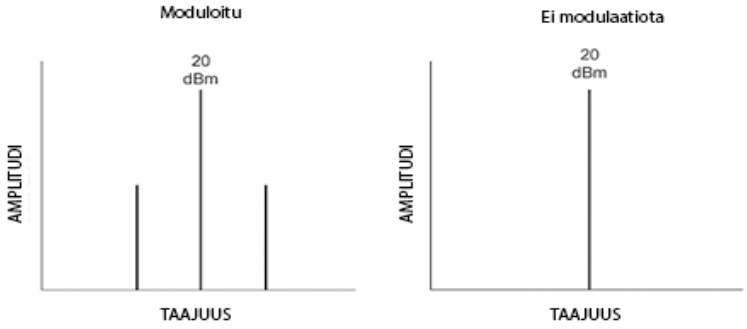
$$V(t) = A\cos(\omega t) \tag{3}$$

missä *A* on signaalin amplitudi, ω on kulmataajuus ja *t* on aika. Signaalin tulkinnan kannalta on hyödyllisempää esittää signaalin tehospektri, josta nähdään signaalin eri taajuuskomponenttien teho. Kuvassa 16 on esitetty yhtälön 3 mukainen yksitaajuuksisen kosinisignaalin tehospektri, missä taajuutta f_c kutsutaan kantoaalloksi.



Kuva 16. *Kosinisignaalin tehospektri, perustuu [1, p. 58].*

Signaali, joka koostuu pelkästään kantoaallosta, ei kuljeta mukanaan informaatiota. Informaatio saadaan lisättyä kantoaaltosignaaliin modulaation avulla. Modulaation seurauksena kantoaallon taajuuden ympärille syntyy uusia taajuuksia. Näiden uusien taajuuksien aluetta kutsutaan sivukaistoiksi ja niihin sisältyy varsinainen siirrettävä informaatio. [2, s. 177] Kuvassa 17 ovat esitettyinä vasemmalla moduloitu ja oikealla ei-moduloitu signaali. Kuvan kantoaallon amplitudi pysyy samana riippumatta moduloinnista tai sen puutteesta. Kuvasta voidaan havaita, että informaatio sisältyy vain sivukaistoille ja modulointi kasvattaa taajuuskaistaa synnyttämällä sivukaistat kantoaallon molemmille puolille [16].



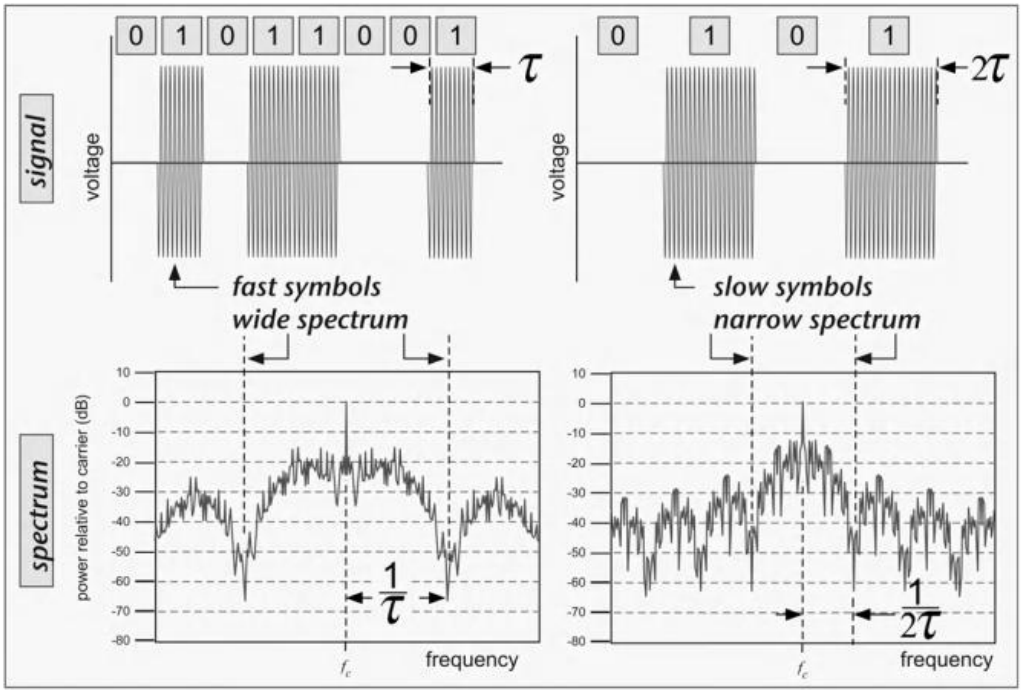
Kuva 17. *Moduloidun ja ei-moduloin signaalin tehospektrit [16].*

4.3 Taajuuskaista

Tietoliikennejärjestelmän tiedonsiirtonopeudella tarkoitetaan sitä, kuinka monta bittiä siirtyy sekuntia kohden. Modulaatiotekniikalla voidaan vaikuttaa symbolinopeuteen, joka puolestaan vaikuttaa bittinopeuteen. Digitaalisen moduulaation tarvitsema taajuuskaista

riippuu pääsääntöisesti symbolinopeudesta ja modulaatiotekniikasta [2, s. 200]. Toisin sanoen, jos signaalia moduloidaan käyttämällä hyvin lyhytkestoisia symboleita, tiedonsiirtonopeus kasvaa, mutta myös järjestelmän käyttämä kaistanleveys kasvaa.

Kuvassa 18 esitetty modulaation kaistanleveyden kääntäenverrannollisuus symbolin kestoon *t*, jossa lyhytkestoisempi symboli kasvattaa kaistanleveyttä 1/t. Kuvassa yksi symboli vastaa nyt yhtä bittiä. Bittijono on kuvattu kantoaallossa vasemmalla lyhyempinä pätkinä, joka näkyy alhaalla olevassa tehospektrikuvassa laajempana kaistana. Oikeanpuoleisessa signaalissa symbolin kesto on ajallisesti kaksinkertainen, jolloin syntynyt kaista on puolet vasemmanpuoleisesta signaalista.



Kuva 18. *Kaistanleveyden suhde symbolinopeuteen [1, s. 60].*

Kaistanleveyden merkitys on olennaista langattomassa siirtotiessä, jossa useampi signaali on läsnä samanaikaisesti. Virheetöntä tiedonsiirtoa varten on olennaista, että toisen järjestelmän signaalit eivät sekoitu muiden järjestelmien taajuuskaistojen päälle. Eri järjestelmille on tyypillisesti valtiokohtaisesti määrätty käytettäväksi eri taajuusalueet, joilla järjestelmien tulee operoida. Lisäksi jotkin taajuusalueet ovat luvanvaraisia tai kiellettyjä kuluttajakäytöltä, joten taajuuskaistan käyttäjän on oltava tarkkana, että laitteisto ei häiritse muita taajuuksia.

4.4 Määräykset

Radioviestintä on valtiokohtaisesti määräyksien alaista. Järjestelmän käyttämällä taajuuskaistalla on väliä, koska maittain on asetettu rajataajuudet joilla tietyt laitteet ja

järjestelmät saavat operoida. Kansainvälinen sääntely kattaa radiotaajuudet 9 kHz:n ja 3000 GHz:n välillä. Kuvassa 19 on esitetty Suomen liikenne- ja viestintäviraston määräyksessä määritellyt RFID-järjestelmän sallitut taajuuskaistat UHF-taajuuksilla, jotka eivät tarvitse radiolupaa tai rekisteröintiä [17].

17 § Etätunnistuslaitteet (RFID)[22]

865,000–865,600 MHz	Efektiivinen säteilyteho ≤ 100 mW ERP. Kanavanleveys 200 kHz[23].
865,600–867,600 MHz	Efektiivinen säteilyteho ≤ 2 W ERP. Kanavanleveys 200 kHz[23].
867,600–868,000 MHz	Efektiivinen säteilyteho ≤ 500 mW ERP. Kanavanleveys 200 kHz[23].
865,000–868,000 MHz	Lukijalaitteen taajuuskaistat: 865,600–865,800 MHz 866,200–866,400 MHz 866,800–867,000 MHz 867,400–867,600 MHz Lukijalaitteen efektiivinen säteilyteho ≤ 2 W ERP.
916,100–918,900 MHz	Lukijalaitteen keskitaajuudet: 916,300 MHz 917,500 MHz 918,700 MHz Lukijalaitteen efektiivinen säteilyteho ≤ 4 W ERP. Kanavaleveys ≤ 400 kHz.
2446,0–2454,0 MHz	Efektiivinen säteilyteho ≤ 500 mW EIRP. Efektiivinen säteilyteho ≤ 4 W EIRP ainoastaan sisätiloissa ja toimintasuhde oltava ≤ 15 %[24].

Kuva 19. *Suomen liikenne- ja viestintäviraston asettamat taajuudet RFID järjestelmälle, joilla voi liikennöidä ilman erillistä lupaa [17].*

Radiotaajuudella kommunikoivien laitteiden pysyminen niille varatulla taajuuskaistalla on tärkeää. UHF RFID -lukulaite ja radiolla varustetut aktiivitunnisteet kommunikoivat radiotaajuuksilla ja näin ollen ovat radiolähettimiä. Radiolähettimet vaikuttavat peittoalueellansa muiden radiolähettimien toimintaan ja vuorovaikutus saattaa ilmentyä haitallisena häiriönä, siirtokapasiteetin tai laadun heikentymisenä [17].

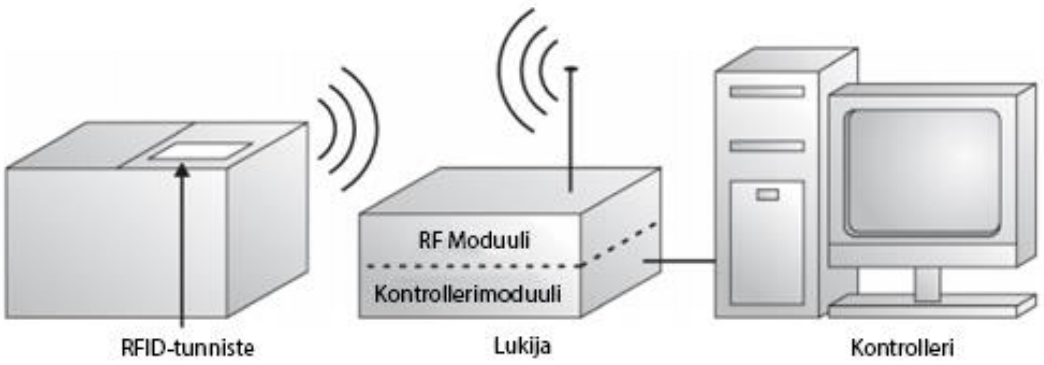
5. UHF RFID -TEKNOLOGIA

RFID tarkoittaa radiotaajuista tunnistamista. RFID-järjestelmän tarkoituksena on tunnistaa ja yksilöidä kohde etäältä, hyödyntämällä tunnistettavaan kohteeseen kiinnitettyä RFID-tunnistetta. RFID-tunnisteen tunnuksen etälukemisen lisäksi tunnisteeseen voidaan tallentaa mitä tahansa kohteeseen liittyvää informaatiota, kuten sarjanumeroita, tuotekuvauksia, konfigurointiohjeita tai aikaleimoja. Optiset tunnistejärjestelmät, kuten viivakoodiin perustuvat järjestelmät, tarvitsevat näköyhteyden kohteen tunnistamiseen. RFID-järjestelmä toimii radiotaajuuksilla, jolloin kohteen tunnistamiseen ei tarvita suoraa näköyhteyttä. RFID-järjestelmän soveltuvuus käyttötarkoitukseensa riippuu järjestelmän käyttämästä taajuusalueesta. UHF RFID -järjestelmät ovat yleisiä hyödykkeiden seurannassa toimitusketjussa [15, s. 7].

RFID-tunnisteet ovat tyypillisesti helppo kiinnittää seurattaviin kohteisiin, sekä tunnisteita voidaan käyttää uudelleen. Tunnisteet voidaan rakentaa iskunkestäviksi ja suunnitella käytettäväksi ympäristöihin, joissa esimerkiksi kosteus, lika tai lämpötila aiheuttavat haasteita. RFID-järjestelmään voi olla kytketty useampi lukija ja yksi lukija kykenee lukemaan usean tunnisteen samanaikaisesti, jolloin saadaan kerättyä suuri määrä dataa nopeasti [15, s. 2].

5.1 UHF RFID -järjestelmä

RFID-järjestelmän perusrakenne koostuu tunnisteesta, lukijasta ja kontrollerista [7, s. 5]. Kuvassa 20 on esitetty RFID-järjestelmän perusrakenne. Seurattavaan esineeseen, kuten pahvilaatikkoon, on liitetty sen yksilöivä tunniste, eli transponderi tai tunniste. Lukijan ja tunnisteen välinen liikenne tapahtuu radioaalloilla. Tunnisteen tieto siirtyy lukijalta kontrollerille, joka on tyypillisesti PC tai palvelin. [7, s. 10]

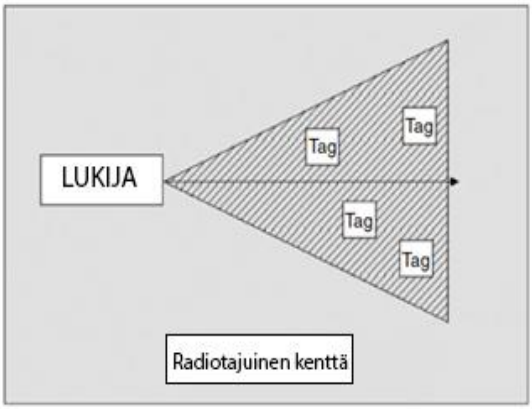


Kuva 20. *RFID-järjestelmän peruskomponentit [7, s. 6].*

Kontrollerit saavat dataa usealta lukijalta ja hoitavat varsinaisen informaatioon liittyvät toiminnot. Toimintoja ovat esimerkiksi inventointi, tietokantaan tallentaminen, kohteiden ohjaaminen, identiteetin todentaminen ja kulkuoikeuksien myöntäminen.

5.2 UHF RFID -tunniste

RFID-tunniste, ts. tagi, on pienikokoinen laite, jonka käyttötarkoitus on yksilöidä ja pitää tallessa informaatiota esineestä, johon se on liitetty. Tunnisteen tiedonsiirto toimii radioaalloilla, joten ne eivät tarvitse suoraa näköyhteyttä lukijan ja itsensä välillä [18, s. 162]. Yksittäinen lukija pystyy lukemaan usean tunnisteen samanaikaisesti, mitä on havainnoitu kuvassa 21.



Kuva 21. *Havainnekuva yhden lukijan ja usean RFID-tunnisteen yhteydestä [18, s. 162].*

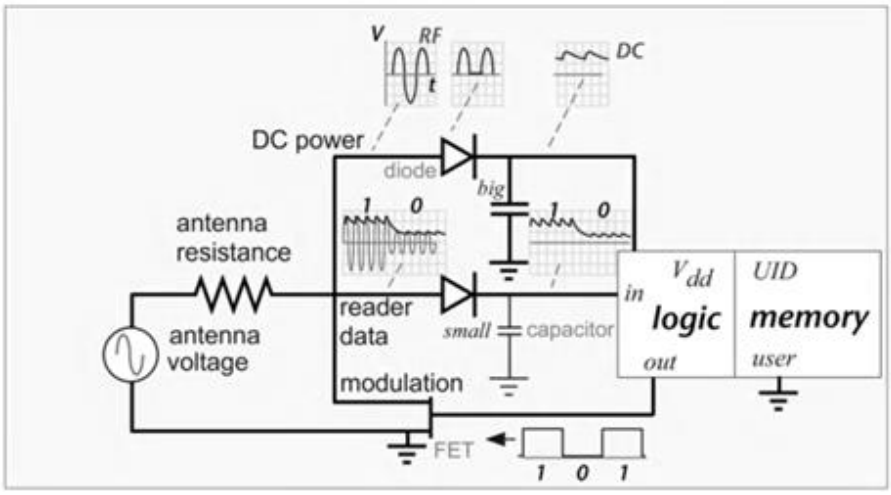
Tunnisteet voidaan jaotella niiden tehonkäytön perusteella. Tunnisteita, joissa on oma virtalähde ja radiolähetin, kutsutaan aktiivisiksi tunnisteiksi. Passiiviset tunnisteet ovat rakenteeltaan yksinkertaisia sekä halpoja ja ne saavat energian toimintaansa varten täysin lukulaitteen lähettämästä sähkömagneettisesta säteilystä. Semipassiiviset

tunnisteet käyttävät teholähteenä paristoja, mutta samalla hyödyntävät lukulaitteen lähettämän signaalin energiaa passiivisen tunnisteen tavoin. [1. s, 33].

5.2.1 Passiivitunniste

Passiivitunniste on tyypillisesti halvin ja rakenteeltaan yksinkertaisin tunnistetyyppi, jonka tärkeimmät, ja joskus ainoat, komponentit ovat antenni ja mikrosiru. Passiivitunnisteet ovat yksinkertaisuudensa vuoksi halpoja ja pieniä, eivätkä tarvitse jatkuvaa huoltoa, mutta verrattuna aktiivi- tai semipassiivitunnisteisiin, niillä on rajoittuneempi laskentakyky ja lukuetäisyys. Passiivitunnisteissa ei ole omaa teholähdettä, vaan ne saavat kokonaan tarvitsemansa energian lukulaitteen lähettämästä signaalista [18, s. 28].

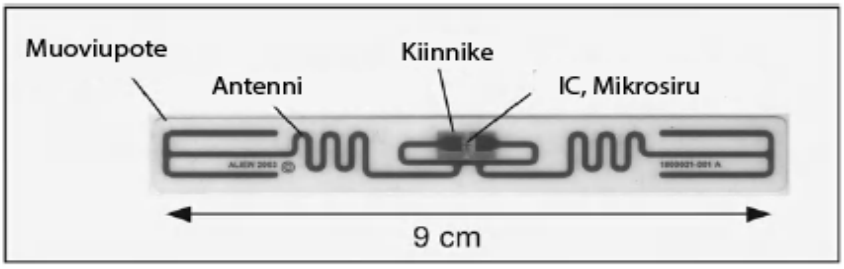
Kuvassa 22 on esitettynä yksinkertaistettu passiivisen tunnisteen piirikaavio. Kuvan piirikaaviossa antenniin indusoitunut energia on mallinnettu jännitelähteenä ja antenni vastuksena. Piirikaavion ylempi diodi ja kondensaattori tasasuuntavat radiotaajuisen vaihtosignaalin tasajännitteeksi, joka antaa käyttöjännitteen logiikkalohkolle. Logiikkalohko lukee antennin vastaanottaman datan diodin ja kondensaattorin kautta, jotka tasasuuntaavat vastaanotetun signaalin, jolloin jännitetasot voidaan lukea loogisena ykkösenä tai nollana. [1, s. 35] Piirikaaviokuvassa logiikkalohkon lähdön bittisekvenssi ohjaa FET-transistorin kantaa, joka puolestaan ohjaa antennin läpi kulkevaa virtaa. Antennipiirissä kulkeva sähkövirta synnyttää lukijalle takaisinsiroavan signaalin, johon informaatio sisällytetään hyödyntämällä ASK-modulaatiota katkomalla antennipiirin läpi kulkevaa virtaa . [1, s. 36].



Kuva 22. *Yksinkertaistettu RFID-passiivitunnisteen piirikaavio [1, s. 35].*

Passiivitunnisteen muistin on oltava ei-haihtuvaa, eli tiedon on pysyttävä tallessa ilman käyttöjännitettä. Logiikkamoduulina käytetään IC:tä (engl. Integrated Circuit), eli mikrosirua. Mikrosirun keskeisimmät tehtävät ovat informaation tallentaminen ja prosessointi, sekä radiosignaalin modulointi ja demodulointi. Sirulta vaaditaan hyvää toimintakykyä korkeilla taajuuksilla. UHF RFID -järjestelmissä käytettyjä siruja ovat esimerkiksi TI CC1101 ja TI CC2533. [19, s. 310]

Kuvassa 23 on esitettynä tyypillinen kaupallinen passiivitunniste (Alien Technology malli 9238 'Squiggle'). Antenni ja siru on kiinnitetty substraattiin tai muoviin. Systeemin päälle asetetaan päällyskerros suojaamaan ja lujittamaan rakennetta [7, s. 9]. Antennina on mutkitteleva dipoliantenni. Tunniste on helposti liitettävissä seurattaviin esineisiin, eikä se ohuen rakenteen ansiosta vaikuta seurattavan esineen dimensioihin.



Kuva 23. *Passiivitunnisteen rakenne [1, s. 37].*

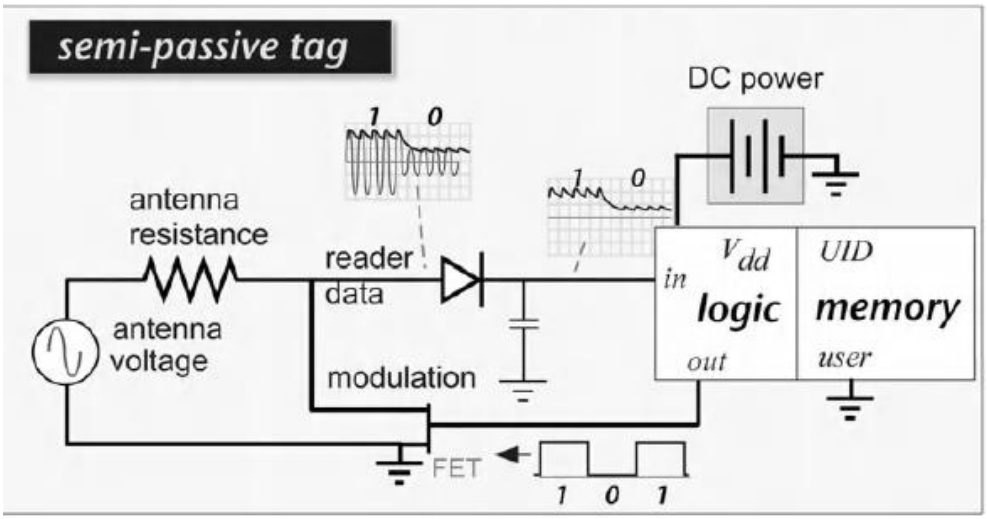
Usein substraatissa on liimapinta, jolloin tunniste pystytään kiinnitämään helposti seurattavaan esineeseen, kuten esimerkiksi pahvilaatikon sivuun [7, s. 20]. Kuvassa 24 on nauha passiivisia liimattavia RFID-tunnisteita.

Kuva 24. *Nauha liimattavia passiivisia RFID-tunnisteita [20].*

Liimattavat passiivitunnisteet ovat halpoja, mutta eivät välttämättä sovellu haastaviin ympäristöihin, missä lämpötilat, mekaaniset iskut ja kosteus aiheuttavat rasitusta tunnisteille. Haastaviin ympäristöihin on saatavilla koteloituja ja kestävämpiä passiivitunnisteita, mutta kappalehinta on korkeampi [21].

5.2.3 Semipassiivitunniste

Semipassiivitunnisteen toimintaperiaate on lähes sama kuin passiivitunnisteen, mutta semipassiivitunnisteella on käytössään oma tasavirta-, eli DC-teholähde (engl. Direct Current). Semipassiivitunniste hyödyntää passiivitunnisteen tavoin takaisinsirontaa lukijan kanssa kommunikoimiseen. [1, s. 36] Semipassiivitunnisteet ja passiivitunnisteet käyttävät usein samaa Gen 2 -protokollaa, jolloin semipassiivitunnisteita voidaan lukea passiivitunnisteiden lukijoilla [21]. Kuvassa 25 on yksinkertaistettu rakennekuva semipassiivitunnisteelle. Rakenne ja toiminta ovat samat kuin passiivitunnisteella, mutta radiosignaalin tasasuuntaamista DC-jännitteeksi oleva piiri on korvattu DC-teholähteellä.



Kuva 25. *Yksinkertaistettu semipassiivitunnisteen kaaviokuva [1, s. 37].*

Oman teholähteen ansiosta semipassiivitunniste kykenee pitempiin, jopa noin 100 metrin lukuetäisyyksiin. Passiivitunnisteisiin verrattuna semipassiivitunnisteet vastaavat luotettavammin lukijan kyselyihin ja toimivat paremmin sähkömagneettisille signaaleille haasteellisissa ympäristöissä [1, s. 36]. Teholähteen ansiosta tunnisteen mikrosiruna voidaan käyttää yleisiä kaupallisia IC-toteutuksia passiivitunnisteille tehtyjen erityisten toteutuksian sijaan [1, s. 37]. Kuvassa 26 on kaupallinen semipassiivitunniste, joka on ollut käytössä yhdysvalloissa tiemaksujen tullauksessa autoihin kiinnitettynä ja sillä on 10 metrin lukuetäisydeellä noin 95% todennäköisyys onnistuneelle lukutapahtumalle [1, s. 37]. Tunnisteen rakenteen dimensioille suurimpana tekijänä on virtalähteenä käytetty paristo.

Kuva 26. *Tietullijärjestelmän (Fastrak) semipassiivitunniste [1, s. 37]*

Koska semipassiivitunnisteen toiminta ei riipu lukijan lähettämästä herätesignaalista, semipassiivitunnisteisiin voidaan liittää sensoreita jotka saavat käyttöjännitteensä tunnisteen virtalähteestä [18, s. 4]. Kuvassa 27 on UHF-semipassiivitunniste, johon on rakennettu lämpötilan mittausta varten lämpötila-anturi ja lämpötilan kirjaaminen.

Kuva 27. *UHF RFID semipassiivitunniste lämpötila-anturilla [22].*

Esimerkiksi kylmiökäytössä semipassiivitunnisteesseen liitetyllä lämpötila-anturilla voidaan seurata siihen kiinnitetyn elintarvikkeen lämpötilaa. Oman teholähteen ansiosta sensorin virta ei katkea tai ole riippuvainen lukulaitteen lähettämän signaalin läsnäolosta, jolloin kylmäketjun katkeaminen voidaan havaita helpommin kun tunniste kykenee jatkuvasti lukemaan lämpötilaa. [18, s. 4]

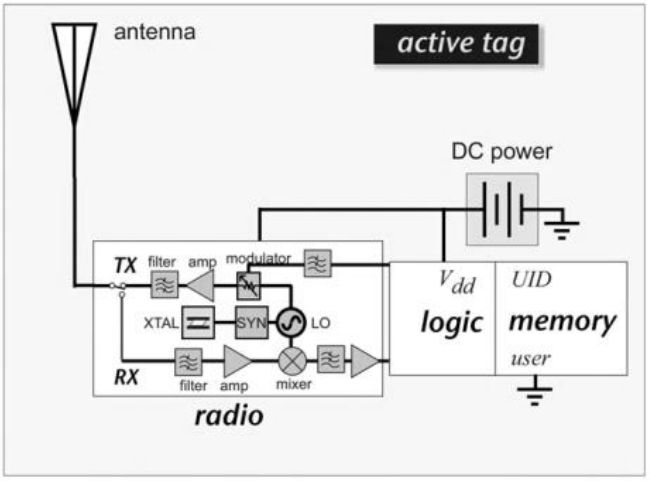
5.2.2 Aktiivitunniste

Aktiivitunnisteet ovat rakenteeltaan monimutkaisempia ja kalliimpia, mutta tarjoavat huomattavasti kehittyneempiä signaalinkäsittelyyn liittyviä toimintoja kuin passiivitunnisteet [18, s. 4]. Aktiivitunnisteissa on oma teholähde, aktiivinen radiolähetin ja vastaanotin. Ne pystyvät vastaanottamaan ja lähettämään signaalin jopa usean sadan metrin tai jopa kilometrin etäisyydellä. [1. s, 38]

Monimutkaisesta rakenteesta johtuen aktiivitunnisteet ovat passiivitunnisteisiin verrattuna isompia, painavampia ja kalliimpia. Lisäksi teholähteenä käytetään tyypillisesti paristoja, jotka aiheuttavat huoltotoimenpiteitä vaihdon takia. Kuvassa 28 on junavaunuun kiinnitetty aktiivinen tunniste, jonka dimensiot ovat huomattavasti suuremmat kuin passiivisen tunnisteen [23].

Kuva 28. *Koteloitu UHF RFID-aktiivitunniste junavaunuun kiinnitettynä [23].*

Kuvassa 29 on esitettynä yksinkertaistettu rakennekaavio UHF RFID -aktiivitunnisteelle. Kaaviosta nähdään, että suurimpana erona aktiivitunnisteen ja passiivitunnisteen välillä on aktiivitunnisteen oma radiokomponentti ja tasajännitelähde. Aktiivisen tunnisteen radiokomponentin ansiosta se pystyy suorittamaan kehittyneempää signaalinkäsittelyä passiiviseen verrattuna.



Kuva 29*. UHF RFID-aktiivitunnisteen yksinkertaistettu piirikaavio [1, s. 38].*

Aktiivitunniste pystyy toteuttamaan taajuusjakoista multipleksausta [1, s. 67]. Tämä tarkoittaa, että radion syntetisaattorilla voidaan luoda kantoaaltosignaali halutulla taajuudella, jolloin useampi lähekkäin sijaitseva tunniste pystyy keskustelemaan eri

taajuuksilla häiritsemättä toistensa viestejä. Lisäksi aktiivitunniste pystyy käyttämään kehittyineitä modulaatiotekniikoita, kuten PSK, FSK ja 16-QAM. Paremman yhteydenhallintaan liittyvien toimintojen ansiosta aktiivitunnisteet toimivat hyvin haastavissakin tiloissa. Haastava tila etätunnistamiselle voi olla varasto, missä metallikontteihin liitetyt tunnisteet ovat sijoitettuna lähekkäin toisiaan ja lukijan ja tunnisteen näköyhteys on estynyt. [1, s. 38]

5.2.4 UHF RFID -tunnisteiden hinta

Tunnisteen yksikköhinnan tulisi olla alhaisempi kuin seurattavan tuotteen, joten tunnisteita valittaessa on tehtävä kompromisseja hinnan, koon ja signaalinkäsittelyyn liittyvien toimintojen, kuten autentikoinnin ja lukuetäisyyksien välillä. Järjestelmän huoltokustannusten lisäksi suuria kappalemääriä seurattaessa varsinkin tunnisteen kappalehinnalla on suuri vaikutus seurantajärjestelmän kustannuksissa. Tunnisteen hintaan vaikuttaa oleellisesti sen koko, sovelluskohde, vaaditut toiminnot, muistin määrä ja suojakotelointi.

Passiivitunnisteet ovat tyypillisesti yksinkertaisesta rakenteestaan johtuen halvimpia kaikista tunnistetyypeistä. Muoviin liitetyt liimattavat tunnisteet maksavat tyypillisesti kappaleelta noin 0,08 euroa ja suojakoteloitujen hinta voi vaihdella välillä 1–20 euroa [24]. Semipassiivi- ja aktiivitunnisteiden kappalehinta vaihtelee välillä 20–100 euroa, riippuen niiden ominaisuuksista ja laitteistosta [25].

5.3 UHF RFID -lukijat

RFID-lukijan tehtävänä on tiedonsiirto itsensä ja RFID-tunnisteiden välillä ja yhä tiedonsiirto tunnisteen ja hallitsevan järjestelmän, eli kontrollerin, välillä. Passiivisen tunnisteen tapauksessa lukija lähettää tunnisteelle sen tarvitseman energian radioteitse. RFID-lukija toimii siis radiolähettimenä ja -vastaanottimena. UHF RFID-lukijat pystyvät lukemaan usean tunnisteen samanaikaisesti. Kehittyneimmät lukijat pystyvät suorittamaan nopeita yhtäaikaisia luku- ja kirjoitusoperaatioita usealle tunnisteelle törmäyksenestomenetelmillä, tunnisteiden todentamista väärinkäytön ehkäisemiseksi, sekä eheyden hallintaa kryptaamalla data. [7, s. 9].

5.3.1 Lukulaitetyypit

Lukulaite voi olla joko paikalleen kiinnitetty tai käsinkannettava. Tyypillisesti käsinkannettavissa lukulaitteissa on sisäänrakennettu antenni, mutta molempia tyyppejä on saatavilla ulkoisilla antenneilla [26]. Varsinkin kannettavalta lukijalta vaaditaan

helppokäyttöisyyttä lukijan painon, koon ja tunnisteiden lukukulmien kannalta, tehokasta virrankulutusta, sekä tarpeeksi korkeat lukuetäisyydet. Lukulaitteen lukualue riippuu sen antenneista. Antenneja voidaan lisätä lukijaan sen portteihin, jolloin lukualuetta voidaan kasvattaa. Tyypillinen määrä antenniportteja yhdellä lukulaitteella on 2, 4 tai 8, mutta suurempia tunnisteiden lukuvolyymejä varten portteja voidaan lisätä käyttämällä multipleksereitä. Kuvassa 30 on esitetty 4 porttinen UHF-lukija. [27]

Kuva 30. *Neliporttinen UHF RFID lukulaite Wi-fi moduulilla [28].*

Usein järjestelmissä useita RFID-lukijoita on sijoitettuna lähekkäin toisiaan. Kuvassa 31 on UHF RFID -lukijoita asennettuna vierekkäin tien yläpuolelle. Lukijat ovat osa tietullijärjestelmää, jossa käyttäjiltä veloitetaan automaattisesti tiemaksu. Käyttäjä tunnistetaan autoissa olevan UHF RFID-tunnisteen avulla. [29]

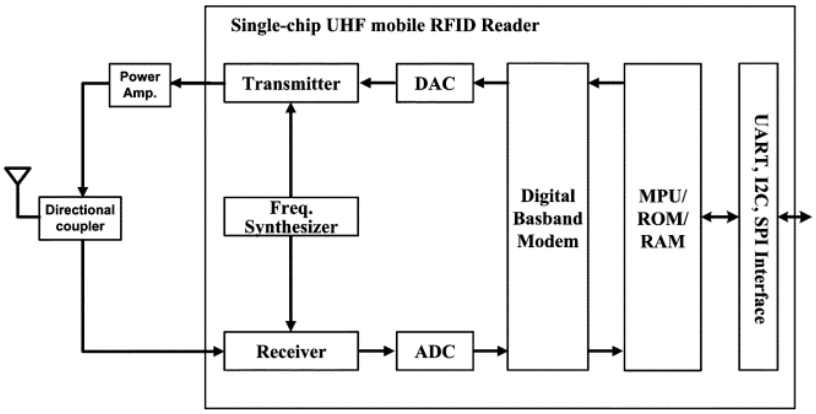
Kuva 31. *UHF RFID-lukijoita tiemaksujärjestelmässä [29].*

Valittaessa RFID-lukijaa on huomioitava lukijalaitteen taajuuskaistat, jotta radiotaajuuksilla toimiminen ei riko maiden radioviestintään liittyviä säädöksiä. RFID-

lukijoiden hinnat vaihtelevat riippuen laitteen lukualeesta, porttien määrästä ja muista ominaisuuksista. UHF RFID-lukulaitteen hinta on tyypillisesti välillä 500 – 2000 $ [30].

5.3.2 RFID-lukijan rakenne

RFID-lukulaite on pohjimmiltaan tutka, jonka keskeisimpinä komponentteina ovat radiolähetin ja radiovastaanotin. Kuvassa 32 on esitettynä kannettavan UHF RFID-lukulaitteen yksinkertaistettu arkkitehtuuri, joka sisältää lähettimen ja vastaanottimen lisäksi, muistilohkon (ROM/RAM, engl. Read-Only Memory / Random Access Memory), rajapinnan ulkoisten järjestelmien kanssa kommunikointiin universaalin asynkronisen lähetin-vastaanottimen (UART, engl. Universal Asynchronous Receiver-Transmitter), kaksisuuntaisen ohjaus- ja tiedonsiirtoväylän (I2C, engl. Inter-integrated Circuit) ja sarjamuotoinen oheislaiteväylä (SPI, engl. Serial Peripheral Interface), digitaali-analogia- ja analogia-digitaalimuuntimet ja tehovahvistimen. Suuntakytkimen tarkoitus on erottaa vastaantuleva ja lähtevä signaali yhden antennin toteutuksissa. [31]



Kuva 32. *Kannettavan UHF RFID -lukulaitteen lohkokaavio [31].*

Lukijan lähetinkomponentilla on kaksi pääasiallista tehtävää, lähettää passiiviselle tunnisteelle sen tarvitsema käyttöteho ja lähetettävän datan tai käskysignaalin modulointi. Vastaanottaessa viestejä tunnisteelta lukijan on lähetettävä ei-moduloitua jatkuva-aikaista signaalia, johon tunniste pystyy moduloimaan viestinsä ja jonka se lähettää takaisinsironnalla takaisin lukijalle**.** Lukijan lähetinkomponentti on kriittinen osa lukijan toimintakykyä ja siltä vaaditaan erityisesti tarkkuutta ja tehokkuutta. Lisäksi lähetinkomponentin on pystyttävä toimimaan ja vaihtelemaan nopeasti kommunikoinnissa käytettyjen eri taajuuksien välillä ja pysyttävä radiotaajuuksien alueella, missä operointi ei mene luvanvaraisille taajuusalueille. [1, s. 155] Lukijan vastaanottimen on pystyttävä erottamaan tunnisteiden lähettämät signaalit muun

radioliikenteen, sekä lähetinkomponentin normaalista toiminnasta aiheutuneiden häiriöiden joukosta [32].

5.4 Standardit

Standardien tarkoitus on edistää laitteiden ja järjestelmien yhteentoimivuutta ja ovat enemmänkin suosituksia, kuin lakivelvoitteisia määräyksiä. RFID-standardit mahdollistavat eri laitevalmistajien laitteiden yhteensopivuuden keskenään. Esimerkiksi jos tunnisteet ja lukijat noudattavat yhdenmukaista standardia, niiden ei tarvitse olla samalta laitevalmistajalta toimiakseen keskenään.

Standardit ja niiden noudattaminen edesauttavat RFID-teknologian kustannustehokkuutta ja RFID-teknologian teollisuuden kasvua parantamalla yhteensopivuutta ja helpottamalla järjestelmien käyttöönottoa. Standardeja tuottavat standardoimisjärjestöt, joista vaikutusvaltaisimmat tahot RFID-teknologian kannalta ovat kansainvälinen standardoimisjärjestö eli ISO (engl. International Organization for Standards) ja EPCglobal [7, s. 87]. Näiden lisäksi on olemassa lukuisia pienempiä standardoimisjärjestöjä, jotka tuottavat RFID-standardeja ja saattavat keskittyä hyvin tarkkaan määriteltyihin yksityiskohtaisiin osa-alueisiin.

Kaupallisissa RFID-tunnisteissa voi usein nähdä mainittavan esimerkiksi termin ”*EPCglobal UHF class 1 Gen 2”.* Tunnisteille on laadittu luokat, jotka on numeroitu yhdestä viiteen. Taulukossa 2 on nimettynä luokat, jotka määritellään tunnisteen toiminnallisuuden perusteella [33].

***Taulukko 2**. EPCglobal RFID-tunnisteluokkia [33].*

Class 0	Passiivinen UHF-tunniste, joka on vain luettavissa. Ohjelmoitu etukäteen sirun valmistuksen yhteydessä. Kommunikointi takaisinsironnalla.
Class 1	Passiivinen UHF- tai HF-tunniste. Muistiin voidaan kirjoittaa vain kerran, mutta lukea useasti. Kommunikointi takaisinsironnalla.
Class 2	Passiivinen tunniste, Kommunikointi takaisinsironnalla. Muistiin voidaan kirjoittaa ja lukea useasti.
Class 3	Semipassiivinen tai passiivinen tunniste. Saattaa sisältää sensoreita oman teholähteen lisäksi.

Class 4	Aktiivitunniste, joka mahdollistaa lisätoimintoja oman virtalähteen ja radiolähettimen ansiosta. Voi kommunikoida muiden tunnisteiden ja lukijoiden kanssa
Class 5	Sama kuin Class 4, mutta pystyy antamaan tehoa muille tunnisteille ja kommunikoimaan muidenkin kuin RFID-lukulaitteiden kanssa.

Termit ”Gen 2” tai ”Gen 1” kertovat, mitä standardeja tunniste noudattaa, joista ”Gen 2” on uudempi. ”Class 1 Gen 2”-tunnisteet ovat takaisinpäin yhteensopivia ”Gen 1 Class 0” ja ”Class 1” -tunnisteiden kanssa. [33]

6. KÄYTTÖKOHTEET JA SOVELLUKSET

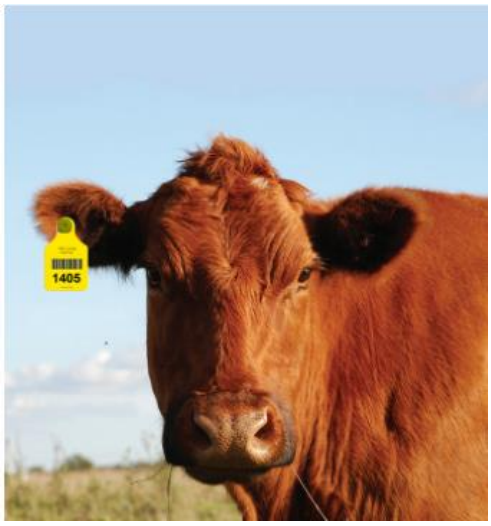
UHF RFID -järjestelmän tarkoitus on vastata tarpeeseen, jossa seurattava kohde on tarkoitus tunnistaa nopeasti ja yksilöivästi etäältä. RFID-teknologialla voidaan ratkaista tunnistustarpeet monessa käyttökohteessa ja ympäristössä. Nykyään UHF RFID-teknologiaa hyödynnetään esimerkiksi lentokoneissa, eläin- ja tuoteseurannassa tietullijärjestelmissä, toimitusketjuissa, reaaliaikaisissa paikannusjärjestelmissä ja kulunvalvonnassa. [34] RFID-järjestelmän käyttöönotto osaksi tuotantoa tai toimitusketjua vaatii resursseja, jolloin RFID-järjestelmää harkitsevan tahon on otettava huomioon käyttökohteensa ja tarpeensa. Oleellisia parametrejä järjestelmän valinnassa on kohteiden määrä, hinta, lukuetäisyys ja ajanjakson pituus, jossa kohde tarvitsee tunnistamista. Esimerkiksi jos aktiivitunnisteen on tarkoitus olla seurattavissa pitkän ajanjakson, sen paristojen vaihtaminen aiheuttaa ylläpitokustannuksia. Järkevän liiketoiminnan näkökulmasta seurattavan kohteen tunnistamisen tulisi tuottaa tarpeeksi hyötyä, jotta etätunnistaminen olisi perusteltavissa. Lähtökohtaisesti seurattavan kohteen arvon tulisi olla suurempi kuin siihen kiinnitetyn tunnisteen. Järjestelmän toteutuksessa on pyrittävä tekemään oikeat kompromissit eri valintakriteerien välillä. Tässä luvussa on esitelty tarkemmin muutamia UHF RFID-käyttökohteita.

Matkustajalentokoneen etätunnistaminen on malliesimerkki etätunnistusjärjestelmän käyttöönoton tuomista hyödyistä ja on perusteltavissa kohteen kappalehinnan ja matkustajien henkien näkökulmasta. Lentokoneen tunnistamisen haasteet liittyvät sen suureen lukuetäisyyteen. Lentokoneissa tunnistaminen on toteutettu koneessa olevalla UHF-transponderilla. Kuvassa 33 on esitetty lentokoneen transponderi. Transponderissa olevat numerot ovat kyseisen koneen 4-bittinen tunniste, joka pystytään asettamaan niiden säätönupeista. Valo kertoo käyttäjälle kun transponderi kommunikoi lukijan kanssa [1, p. 457].

Kuva 33. Yksityiskoneen Squawking 2000 transponderi [35].

Transponderi on aktiivitunniste, joka saa käyttötehonsa lentokoneen moottorin tuottamasta sähköstä. Transponderi pystyy suorittamaan kehittynyttä signaalin käsittelyä, joista tärkeimpänä lentokonesovelluksissa on signaalien törmäyksenesto, jolla vältetään muiden radiosignaalien sekoittumista keskenään [1, p. 457].

Passiiviset UHF RFID-tunnisteet ovat halpoja ja tyypillisesti helposti liitettävissä seurattavaan kohteeseen, joten ne sopivat hyvin sovelluksiin, missä seurattavian kohteiden lukumäärä on suuri, kuten esimerkiksi tuotantokarja tai ihmiset ja kulunseuranta. UHF RFID-järjestelmän etuna muihin RFID-taajuuksiin verrattuna on UHF-järjestelmien kyky lukea usea tunniste samanaikaisesti ja pitempi lukuetäisyys. Esimerkiksi eläinten seurannassa yksittäisen eläimen tunnistaminen on työlästä, joten eläinten tunnistaminen etäältä tehostaa toimintaa. [36] Kuvassa 34 on esitetty UHF RFID-passiivitunniste liitettynä nautaan.



Kuva 34. *Nautaan kiinnitetty UHF RFID-passiivitunniste [37].*

Kirjastoissa hyödynnetään nykyään laajasti ja yhä kasvavassa määrin RFID-teknologiaa inventaarion hallinnassa. RFID-lukuportaaleilla voidaan korvata vanhat sähkömagneettiseen induktioon ja magnetointiin perustuvat hälytysjärjestelmät ja tunnisteet [38]. Tavanomaisten käyttökohteiden lisäksi RFID-teknologiaa voidaan hyödyntää hyvin erityisissä ja innovatiivisissä sovelluksissa. Esimerkiksi RFID-tunnisteista tehty opastus- tai kulkuväylä näkövammaisille, joilla nilkkaan liitetty RFID-lukija suorittaisi opaskoiran tehtävää [39]. Tulevaisuuden käyttökohteista UHF RFID on lupaava teknologia yhdistettäväksi esineiden internetiin (IoT, engl. Internet of Things) tunnistamista vaativiin operaatioihin. RFID:llä voidaan jakaa laitteen yksilöivä tunnistekoodi langattomassa verkossa. [40]

7. HAASTEET JA ONGELMAT

Tavanomaiset haasteet ja epäidealisuuksista johtuvat ongelmat RFID-laitteistolla liittyvät langattomaan radioliikenteeseen. Koska kyseessä on radioliikenteessä tiedonsiirtoa suorittava verkotettu laite, voi RFID-järjestelmä altistua monelle tietoturvaan liittyvälle uhalle. Ihmiset saattavat olla huolissaan luvattomista RFID-lukuoperaatioista, joka ilmenee esimerkiksi kuluttajille myytävissä RFID-suojatuissa lompakoissa. Tässä luvussa on esitelty muutamia RFID-teknologiaan liittyviä ongelmia ja haasteita.

RFID-laitteistot käyttävät mobiililaitteiden tavoin radiokanavaa kommunikointiin. Tästä johtuen RFID-järjestelmät ovat alttiita samankaltaisille tietoturvariskeille ja hakkerointimenetelmille kuin muut elektroniset ja tietoverkossa toimivat laitteet. Tyypilliset hyökkäykset elektronista järjestelmää kohtaan ovat takaisinmallinnus (engl. Reverse engineering), tehoanalyysi, salakuuntelu ja toistohyökkäys, välistävetohyökkäys (engl. Man-in-the-middle attack) ja palvelunestohyökkäys. Takaisinmallinnuksessa hyökkääjä voi lukea RFID-sirulta hänelle kuulumatonta tietoa esimerkiksi purkamalla tunnisteen. Takaisinmallinnus vaatii laajaa ymmärrystä ja osaamista teknologian parista. Tehoanalyysissä hyökkääjä tutkii laitteiston käyttämää tehoa ja voi päätellä siitä hänelle kuulumatonta informaatiota. Hyökkääjä voi salakuunnella hänen hallussaan olevalla luvattomalla RFID-lukijalla tunnisteiden ja lukijoiden kommunikaatiota, jos hänellä on tiedossa käytetyt protokollat ja lukijoiden tiedot. Toistohyökkäyksessä hyökkääjä toistaa järjestelmälle vanhoja oikeellisia viestejä, joita hän on nauhoittanut, saadakseen tietoa tai pääsyn järjestelmään. Välistävetohyökkäyksessä hyökkääjä asettaa oman RFID-laitteensa kaappaamaan järjestelmän viestit RFID-lukijan ja tunnisteen väliltä ja lähettää eteenpäin oman muokatun viestinsä. Palvelunestohyökkäyksessä hyökkääjä estää koko järjestelmän toiminnan, esimerkiksi lähettämällä häiriösignaalia tai fyysisesti tuhoamalla tunnisteet. [41]

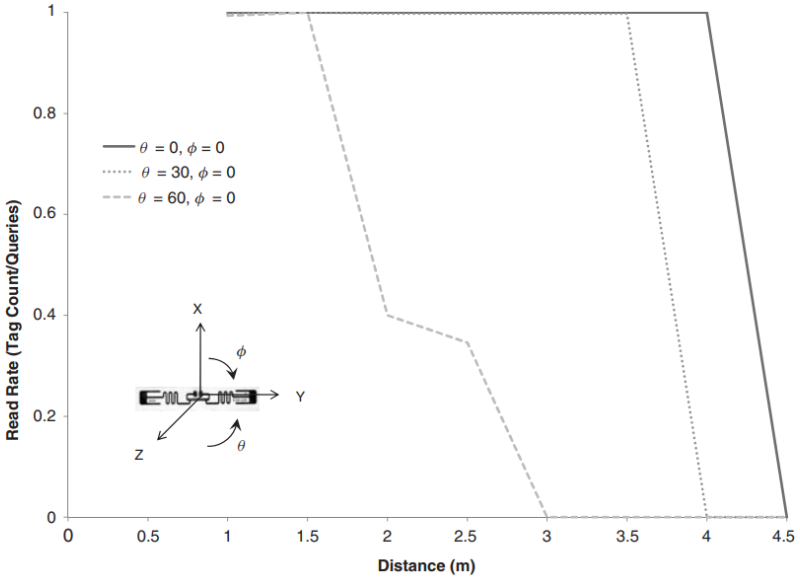
Lukijan ja tunnisteen lukuetäisyys ei ole tarkkaan määritelty, vaan siihen vaikuttaa ympäristön vaikutukset sähkömagneettisen säteilyn käyttäytymiselle. Käytännön sovelluksissa ei siis voida määritellä täysin tarkasti lukualueen etäisyytä ilman mittauksia. Kappale, johon tunniste on kiinnitetty, saattaa vaikuttaa tunnisteen toimintaan. UHF RFID-järjestelmillä ongelmana on sähkömagneettisen säteilyn käyttäytyminen kohdatessaan metallin tai nesteen, sillä neste ja metalli vaimentavat signaalia ja voivat jopa aiheuttaa signaalin taajuuden muutoksia (engl. detuning). Esimerkiksi sähkönjakeluverkkoon liittyvä infrastruktuuri asettaa RFID-järjestelmälle

haastavat olosuhteet, johtuen korkeasta sähköisestä interferenssistä, tyypillisesti metallisista koteloista tehdyistä rakenteista ja vaihtelevasta lämpötilasta ja kosteudesta. [42]

RFID-järjestelmälle oleellista on antennien toiminta, joten yksi isoista haasteista ja kehityskohdista on RFID-laitteissa käytetyt antennit. RFID-järjestelmän toiminnan kannalta yksi kriittisimmistä tekijöistä on antennien suorituskyky. Kehittyineillä antenniratkaisuilla voidaan vaikuttaa antennien suuntaavuuteen ja kokoon. UHF RFID-antennit 900 MHz taajuudella ovat pituudeltaan noin 20 – 30 cm, jolloin tuotantolaitoksessa, jossa voi olla useampia kymmeniä tai jopa satoja lukijoiden antenneja, haasteena on laitteiston koon asettamat rajoitukset. [43]

Tilassa, jossa on useita lukijoita, haasteina ovat antennien suuntaavuuden hallinta, jotta signaalit eivät sekoittuisi keskenään, ja signaalin ylläpitäminen tarpeeksi vahvana RFID-tunnisteiden lukemiselle. Signaalin törmäyksiä (enlg. collision) saattaa aiheutua usean tunnisteen kommunikoidessa lukijan kanssa, kun ne operoivat protokollasta riippuen samalla kanavanvaraukseen liittyvällä tunnisteella. Törmäykset aiheuttavat suurta viivettä lukuoperaatioiden suoritusaikaan. Usea lähekkäin asetettu tunnisteen antenni heikentää lukunopeutta ja lukemisen tarkkuutta, johtuen antennien vaikutuksesta säteilykuvioon, tehonjakautumiseen ja antennien keskinäisimpedanssista. [43]

Tunnisteen ja lukijan suuntaavuus toisiinsa nähden vaikuttaa merkittävästi lukuoperaation onnistumiseen. Kuvassa 35 on UHF RFID-dipoliantennin asennon vaikutus lukuoperaation onnistumiseen kaiuttomassa tilassa [42]. Pystyakselilla on onnistuineiden lukuoperaatioiden suhde kyselyihin, jossa pienempi arvo tarkoittaa useampaa kyselyä ja vaaka-akselilla on lukijan anttennin etäisyys tunnisteesta. Yhtenäinen viiva kuvastaa RFID-tunnistetta, jonka asentoa ei ole muutettu etäisyyden kasvaessa ja katkoviiva kuvastaa tunnistetta, jota on kallistettu 60 astetta.



***Kuva 35**. Antennin asennon vaikutus lukuoperaatioiden onnistumiseen [42].*

Kuvasta nähdään, että kolmen metrin kohdalla kallistettuun tunnisteeseen kohdistuneet lukuoperaatiot ovat epäonnistuneet ja suhdeluku on nolla, vaikka tunniste on vielä lukuetäisyydellä. Erilaisilla antenniratkaisuilla voidaan vaikuttaa asennosta ja suuntaavuudesta johtuviin lukijan ja tunnisteen väliseen kommunikointiongelmiin.

8. YHTEENVETO

Radiotaajuinen etätunnistus on huomattavasti monipuolisempi ja tehokkaampi etätunnistusteknologia verrattuna sitä edeltäviin teknologioihin, kuten viivakoodien optiseen lukemiseen. RFID-passiivitunnisteen lukuetäisyys on huomattavasti korkeampi kuin viivakoodien. Etätunnistus radiotaajuuksilla ei tarvitse näköyhteyttä lukulaitteen ja tunnisteen välillä. UHF RFID-järjestelmä kykenee lukemaan usean tunnisteen samanaikaisesti, mikä mahdollistaa korkeat lukunopeudet. RFID-tunnisteissa on usein muisti, joihin voidaan yksilöivän tunnuksen lisäksi tallentaa muuta tietoa siihen kiinnitetystä esineestä. Lisäksi tunnisteissa voi olla antureita, jotka mittaavat esimerkiksi kiinnitetyn kappaleen lämpötilaa. RFID-tunnuksen muistissa olevaa tietoa on mahdollista muokata jälkikäteen, toisin kuin viivakoodia.

UHF-taajuusalueella toimivat RFID-järjestelmät toimivat tyypillisesti antennin kaukokentässä. UHF-taajuuksien käyttö mahdollistaa muihin taajuusalueisiin verrattuna pitemmän lukuetäisyyden, suuremmat siirtonopeudet sekä pienemmät antennit. UHF RFID-tunniste voi olla joko passiivi-, aktiivi- tai semipassiivitunniste. Aktiivitunnisteella on oma virtalähde ja sisäänrakennettu radiokomponentti mahdollistaen erittäin pitkän lukuetäisyyden ja signaalin käsittelyn. Passiivitunniste on edullisin tunnistetyyppi ja rakenteeltaan yksinkertainen, koostuen tyypillisesti mikrosirusta ja antennista. UHF-taajuuksien käyttäminen mahdollistaa pienemmät ja edullisemmat antennit, joka edesauttaa passiivitunnisteiden käyttöönottoa eri sovelluskohteissa. Kohteen, johon tunniste on kiinnitetty, tulisi olla arvoltaan suurempi kuin käytetty tunniste.

RFID-teknologia on alati kasvava ja lupaava etätunnistusteknologia, joka on jo otettu käyttöön hyvin monella eri toimialalla, joista huomattavimpana käyttökohteena on hyödykkeiden seuranta esimerkiksi varastoissa, satamissa ja tuotantolinjoilla. Lisäksi UHF RFID-teknologialla on huomattavasti mahdollisuuksia erityislaatuisiin innovatiivisiin sovelluksiin.

LÄHTEET

[1] D. Dobkin, The RF in RFID: UHF RFID in Practice, 2nd edition, Newnes, 2012, 540 p.

[2] S. Ellingson, Radio Systems Engineering, Cambridge University Press, 2016, 650 p.

[3] H. Lehpamer, Microwave Transmission Networks, The McGraw-Hill Companies, 2010, 496 p.

[4] H. Young ja R. Freedman, University Physics With Modern Physics, 14th Edition, Global Edition, Pearson Education Limited, 2016, 1600 p.

[5] J. Kraus ja R. Marheka, Antennas for All Applications, Tata McGraw-Hill, 1997, 960 p.

[6] Trafi Viestintävirasto, Rannikkolaivurin radioliikenneopas, Saatavissa (viitattu 20.5.2019): https://www.traficom.fi/sites/default/files/media/file/Rannikkolaivurin_radioliikenneopas.pdf

[7] D. Hunt, M. Puglia ja A. Puglia, RFID - A Guide To Radio Frequency Identification, John Wiley & Sons, Inc, Hoboken, 2007, 240 p.

[8] C. Balanis, Antenna Theory Analysis and Design 3rd Edition, John Wiley & Sons, 2005, 1136 p.

[9] R. Nave, Classification of Polarization, Georgia State University, Saatavissa (viitattu 24.5.2019): http://230nsc1.phy-astr.gsu.edu/hbase/phyopt/polclas.html

[10] Y. Huang ja K. Boyle, Antennas From Theory to Practice, John Wiley & Sonds Ltd, 2008, 378 p.

[11] RFID4U, Dig Deepd RFID tags Construction, Saatavissa (Viitattu 14.4.2019]): https://rfid4u.com/rfid-basics-resources/dig-deep-rfid-tags-construction/

[12] H. W. Silver, The ARRL Handbook for Radio Communications 91st Edition, ARRL, 2013, 1280 p.

[13] D. Christiansen ja C. Alexander, Standard Handbook of Electronic Engineering, 5th edition, McGraw-Hill, 2004, 2200 p.

[14] A. Das, Digital Communication: Principles and System Modeling, Springer, 2010, 246 p.

[15] J. Lahuerte, C. Ripoll, D. Paret ja C. Loussert, UHF RFID Technologies for Identification and Traceability, ISTE Ltd & John Wiley & Sons, Inc, 2014, 192 p.

[16] C. Sayre, Complete Wireless Design, The McGraw-Hill, 2008, 700 p.

[17] TRAFICOM: Liikenne- ja viestintävirasto, Määräys luvasta vapaiden radiolähettimien, Saatavissa (viitattu 24.3.2019): https://www.finlex.fi/data/normit/44836/Maarays_15AO_FI.pdf

[18] S. Ahson ja M. Ilyas, RFID Handbook: Applications, Technology, Security, and Privacy, CNC Press, 2008, 712 p.

[19] A. Eroglu, RF Circuit Design Techniques for MF-UHF Applications, CRC Press, 2013, 358 p.

[20] S. Smiley, ”Active RFID vs. Passive RFID: What’s the Difference?,” RFID Insider, Saatavissa (viitattu 24.3.2019): https://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid

[21] RFID4USTORE, RFID Semipassive Tags, Saatavissa (viitattu 20.5.2019): https://rfid4ustore.com/rfid-tags-labels/rfid-semi-passive-tags/

[22] RFID4USTORE, Caen Temperature Logger UHF Semi Passive Tag, Saatavissa (viitattu 20.5.2019): https://rfid4ustore.com/caen-temperature-logger-uhf-semi-passive-tag/

[23] Confidex Ltd., New Confidex Survivor UHF RFID Tags Deliver Extreme Performance In a Compact Size, Saatavissa (viitattu 24.3.2019): https://www.confidex.com/news-and-events/news/new-confidex-survivor-uhf-rfid-tags-deliver-extreme-performance-compact-size

[24] AtlasRFIDstore, What is RFID? The Beginners Guide to RFID Systems, Saatavissa (viitattu 24.3.2019): https://www.atlasrfidstore.com/rfid-beginners-guide/?utm_source=Quick-Start&utm_medium=Link&utm_campaign=Content&utm_content=Basics-Guide#rfidtags

[25] RFID Journal, Emerald Expositions LLC, Saatavissa (viitattu 24.3.2019): https://www.rfidjournal.com/faq/show?85

[26] AtlasRFIDStore, An intro to RFID Readers, Saatavissa (viitattu 24.3. 2019): https://www.atlasrfidstore.com/an-intro-to-rfid-readers-basic-options-and-features/

[27] M. Kivikoski, L. Sydänheimo ja L. Ukkonen, Read Range Performance Comparison of Compact Reader Antennas for a Handheld UHF RFID

Reader, 2007 IEEE International Conference on RFID, Grapevine, Texas, USA, 2007, pp. 63 –70. Saatavissa (viitattu 24.3.2019): https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4143512.

[28] AtlasRFIDStore, Thingmagic M6 UHF RFID Reader, Saatavissa (viitattu 24.3.2019): https://www.atlasrfidstore.com/thingmagic-m6-uhf-rfid-reader-4-port-wi-fi

[29] S. Lockhart, ISO Standard Aids Interoperability and Data Security, ITS International, Saatavissa (viitattu 26.5.2019): https://www.itsinternational.com/categories/detection-monitoring-machine-vision/features/iso-standard-aids-interoperability-and-data-security/

[30] Emerald Expositions, RFID Journal FAQ, Saatavissa (viitattu 24.3.2019): https://www.rfidjournal.com/faq/show?86

[31] B. Heemunn, K. Choi, J. Sangyoon, Y. Eo, I. Kwon, H. Lee, D. Lee ja S. J, ”A Single-Chip CMOS Transceiver for UHF Mobile RFID Reader, IEEE Journal of Solid-State circuits, vol 3 No 3, 2008, pp. 729 –738. Saatavissa (viitattu 24.3.2019): https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4456779

[32] K. Wang, C. Zhang, Y. Zhang, X. Ji, Y. Zhang, F. Yuan ja Y. Guo, A Monolithic UHF RFID Transceiver for Mobile UHF RFID Readers, International Conference on Integrated Circuits and Microsystems (ICICM), Chengdu, China, 2016, pp 154 –158. Saatavissa (viitattu 24.3.2019): https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7813583

[33] Bar Code Graphics Inc, RFID Tags, Saatavissa (viitattu 22.5.2019): https://www.epc-rfid.info/rfid_tags

[34] Atlas RFID Solutions Store, RFID Beginners Guide, Saatavissa (viitattu: 20.4.2019): https://www.atlasrfidstore.com/rfid-beginners-guide/#introduction

[35] H. Baumeler, Wikipedia Commons, Saatavissa (viitattu 13.4.2019): https://commons.wikimedia.org/wiki/File:Transponder_in_Private_Aircraft.jpg

[36] C. Swedberg, RFIDJournal, Saatavissa (viitattu 22.5.2019): https://www.rfidjournal.com/articles/view?18318

[37] Atlas RFID Solutions Store, Vulcan Custom Animal ID Tag UHF, Saatavissa (viitattu 23.5.2019): https://www.atlasrfidstore.com/vulcan-rfid-custom-animal-identification-tag-uhf/

[38] S. Ching, A. Tai, H. Ip ja L. Fai, The Right UHF RFID Tags for Libraries – Criteria, Concern and Issues, Saatavissa (viitattu 20.5.2019): https://www.intechopen.com/books/designing-and-deploying-rfid-applications/the-right-uhf-rfid-tags-for-libraries-criteria-concern-and-issues

[39] Y. Duroca ja . S. Tedjinib, RFID: A key technology for Humanity, Saatavissa (viitattu 21.5.2019): https://www.sciencedirect.com/science/article/pii/S1631070518300124

[40] A. Sharif ja J. Ouyang, Low-Cost Inkjet-Printed UHF RFID Tag-Based System for IoT applications Using Characteristic Modes, IEEE Internet of Things Journal Vol 6, 2019, pp. 3962–3975. Saatavissa (viitattu 23.5.2019): https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8616825

[41] S. Smiley, 7 Types of Security Attacks on RFID Systems, RFID Insider 2016. Saatavissa (viitattu 25.5.2019): https://blog.atlasrfidstore.com/7-types-security-attacks-rfid-systems

[42] B. Miodrag, D. Simplot-Ryl ja I. Stojmenovic , RFID Systems: Design Trends and Challenges, John Wiley & Sons Ltd, 2010, 576 p.

[43] L. Pui Yi , C. Qingxin ja Y. Wu , Review on UHF RFID Antennas, International Workshop on Electromagnetics: Applications and Student Innovation Competition, London, UK, 2017, pp. 53–55. Saatavissa (viitattu 24.5.2019): https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7968764